

#3

MATTINGLY, STANGER & MALUR, P.C.

JOHN R. MATTINGLY\*  
DANIEL J. STANGER  
SHRINATH MALUR\*

GENE W. STOCKMAN  
Of Counsel

JEFFREY M. KETCHUM  
SCOTT W. BRICKNER  
Registered Patent Agents

\* Bar Membership Other Than Virginia

ATTORNEYS AT LAW  
104 EAST HUME AVENUE  
ALEXANDRIA, VIRGINIA 22301

PATENT, TRADEMARK  
AND COPYRIGHT LAW

FACSIMILE: (703) 684-1157

(703) 684-1120

PRO  
USPTO  
09/645401  
08/25/00

Date: August 25, 2000

Attorney Docket No. H&A-100

To: Assistant Commissioner for Patents  
Washington, D.C. 20231

Sir: Transmitted herewith for filing is the patent application of:

Inventor: Akiko Horiguchi et al (see attached list)

For:  
SHEET-SHAPED MEDIUM, METHOD AND APPARATUS FOR DETERMINATION  
OF GENUINENESS OR COUNTERFEITNESS OF THE SAME, AND APPARATUS  
FOR ISSUING CERTIFICATE

Enclosed are:

- 47 Sheets of Drawings  
 This application is being filed without an executed Declaration.  
 Priority is claimed from Japanese Application No. 2000-180044  
filed June 15, 2000  A certified copy is attached herewith.  
 Copies of the disclosure documents listed on the attached PTO 1449 form and  
 discussed in the specification or  attached Information Disclosure Statement.  
 A verified statement to establish small entity status under 37 CFR 1.9 and 1.27.  
 Specification: Abstract , Description 73 pages; and 14 claim(s).  
 Preliminary Amendment.  
 Executed Declaration.

The filing fee is calculated as shown below:

Small Entity

Large Entity

For:	No. Filed	No. Extra
Basic Fee		
Total Claims	14 -20 =	* 0
Indep Claims	7 - 3 =	* 4
<input type="checkbox"/> Multiple Dependent Claim (s)		

\* If difference is less than zero  
then enter '0' in second column

Rate	Fee
\$ 345	
x 9	\$
x 39	\$
+ 130	\$
Total	\$

Rate	Fee
\$ 690	
x 18	\$ 0
x 78	\$ 312
+ 260	\$ 0
Total	\$ 1,002

A check in the amount of \$ 1,002.00 is enclosed for the filing fee.

The Commissioner is hereby authorized to charge any additional fees that may be required to  
Deposit Account No. 50-1417.

Respectfully Submitted,

By:

John R. Mattingly  
Registration No. 30,293

日本特許庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

JC886 U.S. PTO  
09/645401  
n8/25/00  


別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出願年月日

Date of Application:

2000年 6月15日

出願番号

Application Number:

特願2000-180044

出願人

Applicant(s):

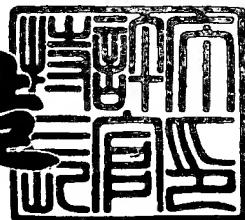
株式会社日立製作所

HORIGUCHI et al  
Mattingly, Stenger & Malin  
703 - 684-1120  
H+A 100

2000年 7月21日

特許庁長官  
Commissioner,  
Patent Office

及川耕造



出証番号 出証特2000-3058351

【書類名】 特許願  
【整理番号】 H000528  
【提出日】 平成12年 6月15日  
【あて先】 特許庁長官 殿  
【国際特許分類】 G06F 17/60  
【発明者】  
【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目280番地 株式会社  
日立製作所 中央研究所内  
【氏名】 堀口 晓子  
【発明者】  
【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目280番地 株式会社  
日立製作所 中央研究所内  
【氏名】 宇佐美 光雄  
【発明者】  
【住所又は居所】 東京都国分寺市東恋ヶ窪一丁目280番地 株式会社  
日立製作所 中央研究所内  
【氏名】 大木 優  
【特許出願人】  
【識別番号】 000005108  
【氏名又は名称】 株式会社 日立製作所  
【代理人】  
【識別番号】 100091096  
【弁理士】  
【氏名又は名称】 平木 祐輔  
【手数料の表示】  
【予納台帳番号】 015244  
【納付金額】 21,000円  
【提出物件の目録】  
【物件名】 明細書 1

【物件名】 図面 1  
【物件名】 要約書 1  
【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 シート状媒体、真贋判定方法、真贋判定装置及び証明書発行機

【特許請求の範囲】

【請求項1】 通信機または通信手段との間で無線通信を行うことによりその内部のメモリに記憶されたデータを無線送信するように構成されたICチップがその一面に取り付けられるか又はその内部に配置され、かつ、その一面には前記ICチップのメモリに記憶されたデータの少なくとも一部を暗号化したものが記されていることを特徴とするシート状媒体。

【請求項2】 通信機または通信手段との間で無線通信を行うことによりその内部のメモリに記憶されたデータを無線送信するように構成されたICチップがその一面に取り付けられるか又はその内部に配置され、かつ、その一面には前記ICチップのメモリに記憶されたデータの少なくとも一部とその媒体に記されている情報の一部とを暗号化したものが記されていることを特徴とするシート状媒体。

【請求項3】 通信機または通信手段との間で無線通信を行うことによりその内部のメモリに記憶されたデータを無線送信するように構成されたICチップがその一面に取り付けられるか又はその内部に配置され、かつ、その一面には前記ICチップのメモリに記憶されたデータの少なくとも一部を暗号化したものが記されているシート状媒体の前記暗号化したデータを読みとて復号化し、復号化したデータと前記ICチップから受信した暗号化前のデータとを照合することを特徴とする真贋判定方法。

【請求項4】 通信機または通信手段との間で無線通信を行うことによりその内部のメモリに記憶されたデータを無線送信するように構成されたICチップがその一面に取り付けられるか又はその内部に配置され、かつ、その一面には前記ICチップのメモリに記憶されたデータの少なくとも一部とその媒体に記されている情報の一部とを暗号化したものが記されているシート状媒体の前記暗号化したデータを読みとて復号化し、復号化したデータと前記ICチップから受信した暗号化する前のデータとの差分データと前記媒体に記されている前記情報の一部とを照合することを特徴とする真贋判定方法。

【請求項5】 外部と無線通信を行うことによりその内部のメモリに記憶されたデータを外部へ送信するように構成されたICチップがその一の面に取り付けられるか又はその内部に配置され、かつ、その一の面には前記ICチップのメモリに記憶されたデータの少なくとも一部を暗号化したものが記されているシート状媒体の前記暗号化したデータを読みとって復号化する手段および復号化したデータと前記ICチップから受信した暗号化前のデータとを照合する手段を有することを特徴とする真贋判定装置。

【請求項6】 外部と無線通信を行うことによりその内部のメモリに記憶されたデータを外部へ送信するように構成されたICチップがその一の面に取り付けられるか又はその内部に配置され、かつ、その一の面には前記ICチップのメモリに記憶されたデータの少なくとも一部とその媒体に記されている情報の一部とを暗号化したものが記されているシート状媒体の前記暗号化したデータを読みとって復号化する手段および復号化したデータと前記ICチップから受信した暗号化前のデータとの差分データと前記媒体に記されている前記情報の一部とを照合する手段を有することを特徴とする真贋判定装置。

【請求項7】 通信機または通信手段との間で無線通信を行うことによりその内部のメモリに記憶されたデータを無線送信するように構成されたICチップがその一の面に取り付けられるか又はその内部に配置されたシート状媒体を保持し、その一の面に証書としての所要事項を記す手段を有することを特徴とする証明書発行機。

【請求項8】 前記ICチップのメモリに所要のデータを書き込む手段を有することを特徴とする請求項7記載の証明書発行機。

【請求項9】 前記ICチップのメモリに所要のデータを暗号化して書き込む手段を有することを特徴とする請求項7記載の証明書発行機。

【請求項10】 前記ICチップのメモリに記憶されたデータを暗号化したものと前記媒体上に記すように構成されたことを特徴とする請求項7記載の証明書発行機。

【請求項11】 前記シート状媒体は紙、プラスチック、シール付きフィルムのいずれか一であることを特徴とする請求項3または4記載の真贋判定方法。

【請求項12】 前記シート状媒体は、生命保険証、傷害保険証、健康保険証、商品券、株券、紙幣、チケット、切符のいずれかの用途に使用されるものであることを特徴とする請求項3または4記載の真贋判定方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明はシート状媒体、真贋判定方法、真贋判定装置、証明書発行機、シート状媒体の正当性判定方法およびシート状媒体のデータ照合方法に関し、特に非接触ICチップを利用した上記媒体、装置および方法などに関する。

【0002】

【従来の技術】

健康保険や車両故障保険、旅行保険などのサービスシステムでは、利用者は紙に書かれた証明書を提示することにより、サービスの提供を受ける資格を証明していた。健康保険の加入者は、保険証を持っていることで健康保険サービスを受けることができた。また、紙幣や商品券は、物やサービスとの交換を行うための貨幣的価値を示す証明書の一種と考えることができる。このように、従来、サービスを受けるためには、印刷技術で偽造防止が図られた証明書が使われていた。

【0003】

サービス全体を管理するサービス機関は、証明書をベースにサービスシステムを運営していた。サービス機関は、利用者から何らかの代償を得ることにより、サービスを受けることができる権利である証明書を提供し、利用者は、実際にサービスを行うサービス実施機関に証明書を提示する、あるいは譲渡することにより、サービス実施機関よりサービスを受けることができた。サービスシステムを管理運営するサービス機関と実際に利用者にサービスを提供するサービス実施機関とは同じ場合もあれば、異なる場合もある。サービス機関とサービス実施機関とが同一のサービスシステムの例として、切符を使った交通システムを挙げができる。鉄道会社などは、切符や定期券などの証明書を利用者に発行し、証明書を保持する利用者に移動のサービスを提供している。また、サービス機関とサービス実施機関とが相違するサービスシステムの例には、健康保険がある。こ

の場合、サービス機関は健康保険組合であり、サービス実施機関は医療機関である。

なお、特開平11-277963号公報には、入場券に非接触ICチップを貼り付け、券面データと同じデータを当該チップ内に書き込むことが開示されている。

#### 【0004】

##### 【発明が解決しようとする課題】

従来の証明書には、いくつかの問題点があった。証明書の中には、少なくとも手のひらサイズほどの大きさがあって持ち運びに不便なことから、通常は家の中に保管されているようなものもある。その場合、利用者が外出先でサービスを受けようと思っても、証明書を所持していないためにサービスを受けられないということが生じる。この問題を解消するために、本来の証明書とは別に、紙あるいはプラスチックできているカード形状の証明書を発行することがあった。しかし、カード形状の証明書の真偽は印刷技術でしか守られていないため偽造の可能性があり、証明書の不正使用を回避するためにサービス機関が別の方法で持ち主確認などを行う必要があり、サービスシステムの運営コストが上昇していた。また、カード状の証明書であっても多くのサービスを受けている場合には枚数が多くなり、携帯に不便であった。

#### 【0005】

カード形状の証明書に限らず、本来の証明書自体も偽造による不正使用の問題をかかえている。貨幣的価値を証明している証明書の一種である紙幣や商品券、株券では、コピー機や高精度の印刷機によって偽造が行われた例がしばしば報道されている。

#### 【0006】

本発明は、証明書あるいは証明書の一部として利用しうる偽造が困難なシート状媒体を提供することを目的とする。また、本発明は、証明書の真贋判定方法、真贋判定装置、シート状媒体の正当性判定方法、シート状媒体のデータ照合方法を提供することを目的とする。また、本発明は、偽造が困難な証明書を発行することのできる証明書発行機を提供することを目的とする。更に、本発明は、証明書の照合をオンラインで行う新規なサービスシステムを提供することを目的とす

る。

### 【0007】

#### 【課題を解決するための手段】

本発明の実施例においては、サービスを実施しているサービス機関の情報、利用者の個別情報、または個々のICチップを識別するユニークな識別情報、あるいはこれらを組み合わせた情報を格納した非接触式のICチップを用いる。このICチップをシート状媒体に実装し、そのICチップが実装されたシート状媒体そのもの、あるいは証明事項が印刷された紙あるいはプラスチック製カード等の媒体にICチップが実装されたシート状媒体を取り付けたものを証明書として利用する。

### 【0008】

本発明の実施例による証明書は、証明書の表面に印刷された情報とICチップのメモリから読み出した情報とを照合することによって証明書の正当性判定を行う。このとき、証明書の表面に印刷された情報とICチップのメモリに格納されている情報を暗号化技術によって結びつけるような構成とすれば、偽造が更に困難になる。あるいは、情報センターのような機関を介在させ、証明書に付いているICチップのメモリから読み出した情報を情報センターに送信して証明書の正当性をオンラインで照会するようなシステムを採用してもよい。

### 【0009】

本発明の実施例によるサービスシステムは、サービスを管理するサービス機関より利用者にサービスの利用権を証明する証明書を配布し、利用者が証明書を提示することにより、サービス機関あるいはその代理機関がサービスを提供するサービスシステムであり、ICチップが組み込まれたシート状媒体が貼られた証明書を使用すること、サービス実施機関では少なくともシート状媒体のICチップの情報を非接触で読み取ることによってそれを提示した利用者にサービスを提供することを特徴とする。上記シート状媒体が貼られた証明書の代わりにICチップが組み込まれたシート状媒体そのものを証明書としてを使用してもよい。ICチップ付きシート状媒体ははがきで配布することができる。サービスを提供するサービス実施機関では、シート状媒体に付いているICチップ内の情報とシート

状媒体の表面あるいはICチップ付き証明書の紙面に表示されている情報を用いてICチップ付きシート状媒体あるいはICチップ付き証明書の正当性を判定し、正当性が証明されたときサービスを提供するようとする。あるいは、ICチップ内に格納された利用権の情報をサービス機関の利用権情報確認センターに問い合わせ、その情報が正当であることを確認することによりサービスを提供する。

#### 【0010】

本発明でいうシート状媒体の用途としては、例えば、次のものが考えられる。

(1) 医療機関などの用途

①検査情報管理、②投薬・検査管理

(2) 家庭などの用途

①振込、送金の用途、②チケット等の予約

(3) 企業などの用途

①社員証、②入室退室管理、③会議室利用、④駐車場の入退場

(4) 店舗などの用途

①売り上げ決済、②購入額に応じた顧客へのポイント発行

(5) 金融機関などの用途

①クレジットカード、②プリペイドカード(例えば、テレフォンカード、鉄道やバスの乗車券の一種)

(6) 物流管理などの用途

①電子伝票、②電子タグ

(7) 交通機関などの用途

①定期券、②乗車券(特急券、座席指定券などを含む)、③搭乗券、④予約券(ホテル宿泊券、コンサートチケットなど)

(8) 公共機関などの用途

①健康保険証、②住民票、③パスポート、④その他ライセンス証(自動車免許証、入場券)

(9) 商品券

#### 【0011】

また、シート状媒体とは、例えば、紙、プラスチック等を素材とした薄いもの

をいう。例えば、商品券、札などがその典型例である。また本発明の実施例の適用対象は必ずしもシート状でなくてもよい。即ち、例えば、うすい板状のものでなくともよい。塊であってもよく、板とはいえない程度の厚さを有していてもよい。シート状であるか否かを問わず、その厚さは均一でも不均一でもよい。平面形状は四角形でも、その他の任意形状でもよい。

すなわち、本発明の実施例によるシート状媒体は、特許請求の範囲の請求項1, 2に記載した通りのものである。

#### 【0012】

ユーザは提供されたICチップ付きシール（シート状媒体）を一定の大きさの窪みが一定間隔で掘られている台紙に貼って保管するのが便利である。シールの上には偽造防止用の印刷を施すことができる。ICチップ付きシールやICチップ付き証明書は、電磁波をシールドする金属膜で覆われた定期入れ等のカードケースに入れて保持するのが安全である。ICチップは、また、台紙をはがすと別なものに貼ることができるシートに装備してもよい。

#### 【0013】

複数のICチップを台紙付きテープ上に一定間隔で実装しておくと、テープをICチップ間の適当なところで切断することによって容易にICチップ付タグを生成することができる。また、外部アンテナと接続された複数のICチップを台紙付きのテープに一定間隔で実装すると、テープをICチップの間で適当なところで切断することによって容易にICチップ付タグを生成することができる。このとき、テープの上に偽造防止用の印刷を施すことができる。ICチップ付きテープの実装は、テープの長手方向に平行に外部アンテナを、ICチップのパッドの間隔と同程度の間隔で離して二つ実装し、平行に置かれた外部アンテナの間にICチップを一定間隔で置き、それぞれの外部アンテナに、ICチップのパッドをそれぞれ接続することによって行うことができる。また、密着実装すると伝導性を持つ導電性粒子を使い、ICチップと外部アンテナの間に導電性粒子を印刷方法で密着して実装することにより、ICチップと外部アンテナを接続するようにしてもよい。

#### 【0014】

本発明の実施例による真贋判定方法は、特許請求の範囲の請求項3，4，11，12に記載した通りである。

本発明の実施例による真贋判定装置は、特許請求の範囲の請求項5，6に記載した通りのものである。

本発明の実施例による証明書発行機は、特許請求の範囲の請求項7～10に記載した通りのものである。

#### 【0015】

本発明の実施例においては、携帯用の証明手段として、非接触ICチップを使用する。印刷技術による証明書は、高性能のコピー機や高精度の印刷装置があれば、偽造できる可能性を否定できない。しかし、ICチップは、半導体製造設備を有する工場でないと製造できないため、印刷技術による証明書に比べて偽造が困難である。ICチップの中に証明に関する情報を格納しておけば、情報を半導体自体の構造によりあるいは暗号技術等で守ることができ、改ざんは極めて困難になる。ICチップは小型であるため、シール状に実装し台紙等に貼り付けることで携帯が容易になり、利用者の利便性が増す。サービス実施機関は、サービスを提供する際にICチップ中の情報を確認することで、より高い信頼性をもってその情報を確認してサービスを提供することができる。

#### 【0016】

ICチップ付きシール（シート状媒体）は薄くて小さいため、配布も容易である。証明書に添付して配布してもかまわないし、はがきを用いて配布することもできる。ICチップ付きシールをはがきで直接配布する方法によると、従来の証明書の配布より低コストで配布することができる。また、証明書の中にICチップを組み込んだり、ICチップを装着したテープを証明書に貼ることにより、証明書自体の偽造も困難にすることができる。これは、先に述べたとおり、ICチップ自体の偽造が、印刷技術に比べて困難であるためである。

#### 【0017】

ICチップ質問機に文字読み取り機能を備えることにより、ICチップ付き証明書のICチップの情報と証明書に記載されている証明情報などの情報を簡単に読むことができるようになる。簡易型証明書発行システムにより、ICチップ付

き証明書が簡単に発行できるようになり、利用者の利便性が向上する。携帯電話にICチップ質問機の機能をつけ、携帯電話とICチップ質問機の機能を兼用させ、質問機のコストを下げることが可能になると同時に、ICチップから読み取った情報を簡単に携帯電話でサービス機関等へ転送することが可能になる。

#### 【0018】

本発明の実施例によれば、小型のICチップ付きシールを証明書の代わりに使うことが可能となり、証明書の携行性が増す。また、ICチップ付きシールやICチップ付き証明書を使うことにより、証明書の偽造を困難にすることが可能になり、サービス機関やサービス実施機関が行うサービスシステムの信頼性を向上させることができる。

#### 【0019】

##### 【発明の実施の形態】

以下、図面を参照して本発明の実施の形態を説明する。

図1に非接触のICチップの構成例を示す。ICチップ102は、アンテナ部104と電源部106、論理部108、メモリ部110からなる。非接触ICチップは、接点を持たず、質問機からアンテナ部104に電波を送ることにより、電源の供給及びクロック、データの送受信を行う。アンテナ部104は、ICチップのチップ内にあるものと、外部にあるものとがある。図1は、チップ内にアンテナ部を持つICチップを想定したものである。チップ外にアンテナ部を持つものは、アンテナ部がチップの外付けになっている。本発明の実施例は、アンテナ部がチップ内にあるかチップ外にあるかに拘わらず、いずれの方式のICチップも利用できる。また、質問機とアンテナ部の間で非接触に情報を送受信する方式として、電磁誘導などいくつかの方式がある。本発明の実施例はいずれの送受信方式のICチップも利用できる。

#### 【0020】

次に、ICチップ102の動作について説明する。まず、アンテナ部104で電波を受け、電源部106でICチップ全体の回路で使用する電源を生成する。アンテナ部104で受けた電波から、クロック成分が取り出され、ICチップ全体の回路のクロックとして使用される。論理部108は、質問機から送られてき

た指令に従い、処理を行う。メモリ部110は、ICチップに記憶すべき情報を格納する領域である。ICチップには、さまざまな方式があり、メモリもROMしかももたない書き換え不可能なタイプから、EEPROMのように電気的に書き換え可能なメモリを持ち、書き換え可能なタイプがある。本発明の実施例においては、これらのいずれの方式のICチップも利用可能である。

#### 【0021】

本発明の実施例では、メモリにサービスを管理運営しているサービス機関に関する情報を格納しているタイプのICチップ、利用者情報を格納しているタイプのICチップ、チップごとに異なった番号が格納されているタイプのICチップ、あるいはそれらを組み合わせた情報を格納しているタイプのICチップを使用する。

#### 【0022】

ICチップは小さく作ることが望ましいため、あるサービス機関が発行するICチップには、そのサービス機関からの発行であることを示す情報を格納するタイプのICチップを用いるのが一つの方法である。このタイプのICチップの場合、同一のサービス機関から発行されるICチップ内の情報はみな同じである。これは、利用者に関する個別情報を持っていないという欠点があるが、ICチップへの情報は一般にROMを使って書き込まれているため、後から改ざんができないという利点がある。また、ROMだけであるのでチップサイズを小さくできる利点がある。利用者情報を格納しないでサービス機関に関する情報を格納するタイプのICチップは、ICチップが添付された証明書等が利用者に依存しない、あるいは利用者が最初から分かっていないものに使うことができる。例えば、商品券やチケット、切符などに使用することができる。

#### 【0023】

サービスを受ける利用者ごとに関する情報を格納するタイプのICチップは、サービス機関が利用者にICチップを提供する際に利用者情報を書き込む必要がある。ICチップに情報の書き込みを行うには、メモリとして書き換え可能なメモリを用いる必要があり、さらに書き換え可能なメモリの制御回路が必要なため、チップサイズが大きくなる可能性がある。利用者情報を格納するタイプのIC

チップは、健康保険や生命保険の証明書や身分証明書など利用者が予めわかっている証明書に用いることができる。

#### 【0024】

別な方式として、ICチップメーカーがICチップを製造する際に、ICチップ毎に異なったユニークな番号をつけ、そのユニークな番号を格納するタイプがある。これは、ICチップに書き換え可能なメモリを持たないため、書き換え可能なタイプに比べてチップサイズが大きくならないという利点がある。ただし、ICチップ製造時に、電子ビーム描画装置などでICチップの一つ一つに個別の番号を書き込む必要がある。電子ビーム描画装置を使えば、メモリ部のROMのヒューズを電子ビームで溶かすことにより、それぞれのICチップに個別の番号を書くことができ、回路内にメモリの書き換え回路が不要となる。チップ毎にユニークな番号が格納されているICチップは、健康保険証など一枚一枚の証明書ごとに異なった番号をつけたい場合に用いることができる。

#### 【0025】

ICチップは、小さなチップであるため、何らかの媒体に組み込まれて使われる。シールにICチップを実装したICチップ付きシール202を横からみた断面を図2に示す。ICチップ204は、2枚のペットフィルム206と210ではさまれ、ICチップと2枚のペットフィルムは、接着剤208で接着されている。ICチップ付きシール202を別なものに貼りやすいように、ペットフィルム210の裏面に粘着剤212がついて、それを保護する台紙214が装着されている。台紙214を剥がすことによりICチップ付きシール202を別のものに容易に貼ることができる。図3は、図2のICチップ付きシール202を上から見た図である。ICチップ204が中央に実装されている。

#### 【0026】

ICチップの実装方法として、テープ状に実装する方法もある。図4は、テープ402にICチップ404や406を組み込んだものを示す概略図である。テープ状に実装した図4のICチップの断面図は図2の断面図と同じである。テープ状の実装の特徴は、粘着テープ（例：セロファンテープ）のように巻いて保存ができるため、運搬や別のものへ装着する加工が容易なことである。証明書等への

ICチップの貼り付けに当たってはテープ402から1個のチップを切り出し、下の台紙を剥がして粘着剤を露出させて貼り付ければよい。

#### 【0027】

ICチップは、図1に示すようにチップ内にアンテナを組み込んだタイプと、チップ外の外部アンテナを使うタイプがある。図1のようにチップ内アンテナを用いる場合は、外部アンテナと接続する必要がないため、シールなどへの組み込みが容易である。しかし、チップ内のアンテナしかないので、質問機とチップとの通信距離が比較的短い場合が一般的である。質問機との通信距離を伸ばすためには、チップ外のアンテナを利用する必要がある。

#### 【0028】

図5に、外部アンテナと接続するパッドを持ったICチップの一例の平面図を示す。502はICチップ全体であり、504は、図1のアンテナ部を除いた、電源部、論理部、メモリ部を実装した部分である。506と508は、外部アンテナと接続するためのパッドである。図5に示したICチップを外部アンテナと接続した状態の平面図を図6に示す。外部アンテナ606と608はテープ602に実装されている。外部アンテナ606と608の間にはギャップがあり、2つのアンテナは電気的に接続されていない状態でテープ602に実装されている。この上にICチップ502を裏返して接続する。接続に当たっては導電性の接着剤などを使用する。ICチップ502のパッド506は一方の外部アンテナ606に接続され、パッド508は他方の外部アンテナ608に接続される。

#### 【0029】

次に、外部アンテナを使うICチップの効率的な実装方法を説明する。外部アンテナとICチップを長いテープ状に実装する例を図7に示す。テープ702には、一定間隔で外部アンテナ708、710、712が実装されている。それらの間はギャップがあり、各アンテナは電気的につながっていない状態である。その上に、ICチップ704、706を置く。ICチップには裏表があるため、必ずパッドが設けられた裏側が下になるようにして置くことが困難であれば、図8に示すようなテープ802に外部アンテナ804、806、808を実装したテープを再度テープ702の上から張りつけ、ICチップ704、706が必ずア

ンテナと接続されるようにする。出来上がったICチップ付きテープは図9のようになる。図9は、上から張り付けたテープ802を剥がした状態を示す。ICチップ704, 706は外部アンテナ708, 710, 712あるいは外部アンテナ804, 806, 808と接続された状態となる。これを、ICチップが一つしかついていないように適当な位置で外部アンテナ部を切断分離し、ICチップ付きタグを作る。一般には、ICチップ付きタグとして使用する。図10に示すICチップ付きタグ1002は、ICチップ1004が実装されており、外部アンテナ1006と1008が接続されたものである。

#### 【0030】

ICチップの裏表を制御しないで自由に置いても、外部アンテナとICチップを後で接続するには他の方法もある。その一つの方法は、図7のテープ702の上から、印刷すると外部アンテナとパッドを接続させるカーボン粒子のような導電性微粒子を吹き付け、ICチップ704や706がパッドの設けられていない表側を下にして貼り付けられても、アンテナと接続させる方法である。実施例を図11に示す。導電性粒子が印刷された部分1114は、ICチップ704と外部アンテナ708を接続する。ICチップ704が裏側を下にして実装されていれば、ICチップの裏面と外部アンテナは既に接続されているため、印刷部分1114は何ら影響を与えない。印刷部分1114, 1116, 1118, 1120はそれぞれ、ICチップと外部アンテナを接続している。インクジェット方式による印刷法は精度良く安価に印刷パターンを制御できるため、インクジェットによって導電性微粒子による印刷部分1114, 1116, 1118, 1120を形成することで、ICチップ付きテープの実装コストを削減する事ができる。

#### 【0031】

ICチップは非常に小さいのが一般的であり、図7の外部アンテナ708と710の間に横方向と縦方向を合わせてICチップを置くことは、制御が複雑になり、コストの上昇を招く。ICチップと外部アンテナを接続するための実装方法として、一つの方向だけ正確に置けばよい実装方法を図12に示す。これは、一つずつに分離されたICチップ付きタグ1002（図10参照）の長さ方向の幅のテープ1202に外部アンテナ1212, 1214を実装し、その間にICチ

ップ1204, 1206, 1208, 1210を接続する方法である。ギャップに合わせて正確にICチップを置く必要があるが、テープに沿った方向1216では、ICチップを置く位置はそれほど正確でなくてもよい。実装する際に、テープが動いている方向のみ正確に合わせるだけでよいので実装が容易になる。ICチップ1204, 1206, …を実装したテープ1202からICチップ付きタグ1002を作るには、テープ1202を横方向に切断すればよい。

#### 【0032】

別の実装方法を図13に示す。テープ1302に、平行に外部アンテナ1308と1310を実装する。その上にICチップ1304, 1306を置き、接続する。各ICチップのパッド506が外部アンテナ1308に接続され、パッド508が外部アンテナ1310に接続される。図12の実施例と同じように、テープの動く方向1312に合わせて、ICチップを正確に置くだけによく、ICチップ1304と1306の間隔はそれほど正確でなくてもよい。図7の実施例と同じように、ICチップが小さいため、裏表の制御が難しい場合は、テープに外部アンテナのみが実装されているものを貼り付ける方法もある。図14は、そのようにして貼り付けた結果を示す図である（図は最上層のテープを剥がした状態を示す）。ICチップ1304と1306は外部アンテナ1308と1408, および外部アンテナ1310と1410で挟まれている。図15は出来上がったICタグ付きテープ1502を示し、ICチップ1504, 1506の表面と裏面は外部アンテナ1508, 1510に接触している。ICチップ1504と1506の間を適当に切断することにより、図16に示すICチップ付きタグ1602ができる。ICチップ1604に外部アンテナ1606と1608が接続されている。

#### 【0033】

ICチップ付きシールのICチップのメモリは書き換えが困難であるため、ICチップを証明に用いる方法は偽造防止に有効な方法である。ICチップのこの特徴を利用し、証明書自体の偽造をより困難にすることができます。

#### 【0034】

図17に、ICチップをテープに実装したICチップ付きテープを貼ることに

より、偽造をより困難にした証明書1702を示す。ICチップ付きテープ1704は、ICチップ1706を実装しており、証明書1702に貼られている。この状態で、ICチップ1706内の情報を質問機で読み出し、その情報が正当であることを確認することによって、証明書1702が本物であるかどうか確認できる。この証明書は、印刷技術で偽造防止を図っていたこれまでの証明書に比べて、簡単に偽造できないICチップを使っているため、偽造をより困難にすることができる。この場合、ICチップに格納する情報は、証明書の証明目的や用途等に合わせて、サービスを管理運営しているサービス機関に関する情報、利用者に関する情報、チップごとのユニークな番号あるいはこれらを組み合わせた情報とする。

#### 【0035】

偽造防止をより確実にするには、ICチップ1706内の情報と印刷情報を組み合わせるのが望ましい。図17に示した方法では、証明書1702を印刷技術で偽造し、別の証明書から取り出したICチップをテープに実装することで、偽造した証明書を作ることが考えられる。たとえば、証明機関に関する情報（同一の情報）が格納されたICチップ付きパスポートがあったとすると、印刷技術でパスポートを偽造し、別のパスポートから取り外したICチップを組み込むことにより偽造することが考えられる。この偽造方法をICチップ成りすまし偽造と呼ぶ。これを防ぐための一つの方法として、ICチップ内の情報を加工した内容を証明書の表面に印字する方法がある。

#### 【0036】

加工の方法として、ICチップ内の情報がチップごとに異なる場合と同じ場合に対して二つの方法がある。ICチップ内の情報がチップごとに異なる場合でも、証明書の表面に記載された情報とICチップ内の情報との間に何ら関連性がない場合は、成りすまし偽造が行われる可能性がある。成りすまし偽造の可能性を減らす方策の一つとして、公開鍵暗号方式を使ってデジタルサインを使用する方法がある。

#### 【0037】

公開鍵暗号方式（あるいは非対称暗号方式とも呼ばれる）の特徴は、公開鍵と

秘密鍵との2種類の異なった鍵を使用することであり、RSAなどが有名である。公開鍵は、暗号文を生成するための鍵であり、一般に公開することが多い。秘密鍵は、暗号文を復号するための鍵であり、非対称暗号の所有者Aが秘密に隠しているものである。公開鍵は公開されているため、Aにデータを送信する場合、データを公開鍵で暗号化して送信することによりデータの隠蔽を行うことができる。Aは、暗号化されたデータを自分の秘密鍵で復号化してデータを取り出す。一方、データxがAが送信したデータであることを証明するためには、データxをAの秘密鍵skで暗号化処理をする（これをデジタルサインと呼ぶ）。その結果を[x] skとする。xと[x] skを受け取ったものは、Aの公開鍵pkを使って、[x] skからx1を取り出し、x1とxが同じであることを確認することにより、データxがAから送られてきたことを証明することができる。

## 【0038】

RSAでの暗号化の方法は、次式(1)のとおりである。

$$y = x^{**e} \bmod n \quad (1)$$

ここで、eとnは公開鍵、xは暗号化するデータ、\*\*はべき乗演算、modは剰余演算である。復号化の方法は次式(2)のとおりである。

$$x = y^{**d} \bmod n \quad (2)$$

ここで、dとnは秘密鍵、yは復号化するデータ、modは剰余演算である。

## 【0039】

一方、RSAでのデジタルサインの生成方法は次式(3)のとおりである。

$$y = x^{**d} \bmod n \quad (3)$$

ここで、dとnは秘密鍵、xはデジタルサインをするデータ、modは剰余演算である。デジタルサインの認証（確認）方法は次式(4)のとおりである。

$$x = y^{**e} \bmod n \quad (4)$$

ここで、eとnは公開鍵、yはデジタルサインされたデータ、modは剰余演算である。

## 【0040】

デジタルサインの利用方法を以下に示す。ICチップ内の情報をサービス機関の秘密鍵でデジタルサイン（暗号化処理）をした結果をICチップ付き証明書に

印刷しておく。ICチップ付き証明書の正当性を確認する際、証明書に印刷されている情報を公開鍵で復号化処理を行った結果がICチップ内の情報と同一になれば、デジタルサインの印刷結果とICチップの対応が取れたことになり、その証明書の正当性を証明することができる。この方法では、紙面上にICチップ内の情報のデジタルサインの結果を印刷する必要があり、印刷上の制約を加えることができるため、偽造がより困難になる。

## 【0041】

さらに、偽造を困難にするための方法として、ICチップ内の情報と証明書の表面に印刷されている重要な情報を組み合わせた結果のデジタルサインを証明書の表面に印刷する方法が考えられる。本方式は、ICチップ内の情報が証明書ごとに異ならなくても偽造防止のために有効である。たとえば、証明書の重要な情報として、パスポートでは氏名、紙幣では金額などの情報がある。同一の情報を格納したICチップを組み込んだだけの証明書、例えば金額の如何によらず全ての紙幣に同じICチップを組み込んだ場合を想定すると、額面1000円の紙幣のICチップを取り外して、10000円の紙幣の中にそのICチップを組み込んだ場合でも、ICチップ成りすまし偽造を防ぐことはできない。ここに提案する方法では、ICチップ内の情報x1と証明書の表面に印刷されている重要な情報x2を使い、次式(5)のようにデジタルサインの結果yを求める。x2は、商品券や紙幣の金額やパスポートでの氏名である。

$$y = (x_1 + x_2)^{\star\star d} \bmod n \quad (5)$$

## 【0042】

ここで、 $x_1+x_2$ の操作は、 $x_1$ と $x_2$ の文字をつなげる操作あるいは文字列を数値に変換して加算する操作を表す。 $x_1+x_2$ の演算結果を短くすると式(5)の処理時間を短縮することができるため、 $x_1+x_2$ の処理結果をハッシュ関数でハッシュした値を $(x_1+x_2)$ の代わりに使うこともできる。証明書には、 $x_2$ と $y$ が印刷される。dは、証明書を発行している機関の秘密鍵である。ICチップ付き証明書の正当性を確認する場合は、dに対応する公開鍵eを使って、次式(6)のzを求める。

$$z = y^{\star\star e} \bmod n \quad (6)$$

## 【0043】

得られた $z$ は、式(5)の $(x_1+x_2)$ に対応し、例えばICチップ内の情報と金額情報である。次に、ICチップの内容を読み込み、 $z$ からICチップの情報を引く。その結果、次式(7)のように金額情報が得られる。

$$x_2 = z - x_1 \quad (7)$$

## 【0044】

$x_2$ が、証明書の表面に印刷されている金額情報と同一であれば、その証明書の正当性が確認される。もし、 $y$ にハッシュした値を使っているならば、式(6)で得られた結果 $z$ が、 $x_1+x_2$ の演算結果（ICチップ内の情報 $x_1$ と証明書の表面に印刷されている重要な情報 $x_2$ を”+”操作した結果）をハッシュした値と同じ結果になっていれば、その証明書の正当性が確認される。

## 【0045】

ICチップの情報と証明書に記載された情報を使って証明書の正当性を確認する方法を、“ICチップ情報と証明書記載情報を使った正当性確認方法”と呼ぶ。ここで説明した例では、公開鍵暗号方式を使ったが、DESのような対称暗号でも同じようなことはできる。ただし、対称暗号鍵を外部にわからないようにする施策が必要である。

## 【0046】

図18に、ICチップ情報と証明書記載情報を使った正当性確認方法の実施例を示す。商品券などの金額情報1804とテープ1806内に格納されているICチップ1810内の情報を秘密鍵で暗号化し、その結果を1808に印刷する。情報1808を公開鍵で復号化すれば、ICチップ内の情報と金額情報に相当する情報が得られる。それらが、実際の情報と同じであれば、この証明書1802の正当性が確認できる。たとえば、この証明書の金額情報1804を1000円に変更しようとしたとしても、偽造者は、秘密鍵を知ることができないため、デジタルサインの結果である1808を求めることができない。従って、金額情報1804だけ偽造したとしても、正当性を確認する際に容易に、ICチップ成りすまし偽造がなされていることが分かる。

## 【0047】

図19は、ICチップ1908を証明書1902に直接貼るあるいは、すき込んだ実施例である。ここで「すき込む」とは、証明書等の媒体が紙である場合、原料から所定の厚さの紙を製造する工程の中で、紙の中にICチップを埋め込んでしまうようなことをいう。金額情報1904とICチップ1908内の情報を合わせたデータのデジタルサインの結果を情報1906として印刷してある。

#### 【0048】

図20は、シール上に情報を印刷した実施例である。この例では、証明書の番号2004とICチップ2008内の情報を合わせたデータをデジタルサインした結果2006をシール2002の表面に印刷してある。なお、ICチップ付き証明書やICチップ付きシールに印刷する情報を、文字以外の例えばバーコードのような機械読み取り可能な情報としても同じように本発明の実施例は適用することができる。また、ICタグ付きシールやICタグ付きタグの偽造防止をさらに困難にするためには、シールやタグの表面にホログラムやアルミ箔を印刷したり貼ったりすることも効果的である。

#### 【0049】

図21は、ICチップ付きシールをはがきに添付し、郵便により配布する方法の説明図である。保険の証明書等は、しばしば郵送によって契約者に届けられる。ICチップ付きシールは紙の証明書に比べて小さいため、ICチップ付きシールだけを送る場合、封書ではなく葉書で送ることができれば、郵送コストの削減が期待できる。本実施例は、二つに折ってビニールで圧着したはがき2102において、はがき内にICチップ付きシール2104を挟み込みこんだものである。また、図22は、直接ICチップ2204をすき込んだはがき2202を使用して、ICチップ付き証明書を契約者に配布する実施例である。また、図23は、証明書2302に台紙付きICチップ付きシール2308を貼ることにより配布する実施例である。この実施例では、証明書を配布すると同時にICチップ付きシールの配布が可能である。証明書2302には、保険会社名2310とともに証明書番号2304とデジタルサインの値2306が印刷され、ICチップ付きシール2308にも証明書番号とデジタルサインの値が印刷されている。

#### 【0050】

ICチップの質問機は、ICチップに電波によってコマンドを送り、ICチップとの間でデータの転送を行うものである。ICチップを証明書に適用する際、携帯電話をICチップの質問機として兼用できれば、ICチップ付き証明書の正当性判定を携帯電話で行うことができるようになり利便性が増す。携帯電話とICチップの質問機を兼用にすることの他の利点は、装置のコストを削減できることである。携帯電話とICチップの質問機とを兼用して使用する例としては、サービスを提供するサービス実施機関が使用する場合と、サービスを受ける利用者が使う場合を考えられる。サービスを提供するサービス実施機関での使用例としては、携帯電話と兼用のICチップの質問機でICチップを持ってきた利用者の正当性の確認を行う場合を考えられる。携帯電話のような機器は店舗などで一般に使われる可能性が高いため、ICチップの質問機と兼用にするとコストを削減したり、機器の専有場所を減らすのに役立つ。サービスを受ける利用者による使用例としては、利用者が持っている携帯電話で、ICチップを使ったサービスを携帯電話経由で受ける場合を挙げることができる。

#### 【0051】

図24は、携帯電話2406をICチップ付きシート2402の質問機と兼用させた実施例の説明図である。ICチップ質問機と兼用する携帯電話機2406には、ICチップの質問機能と携帯電話機能との機能選択スイッチ2412についている。スイッチ2412によって質問機能と携帯電話機能を選択する。

#### 【0052】

ICチップ質問機兼用携帯電話2406の一例の機能ブロック図を図25に示す。この携帯電話には、携帯電話モードとICチップ質問機モードがある。これらのモードはスイッチ部2514によって選択される。ICチップ質問機モードが選択されると、ICチップ用アンテナ部2504とICチップ質問機処理部2526、出入力部2516が接続される。ICチップ情報格納部2530は、ICチップ質問機処理部2526と携帯電話機能処理部2524のどちらにもつながれており、どちらのモードでも使用できる。ICチップ質問機モードでは、ICチップ質問機としての入力は、携帯電話のボタン2410で行われ、出力はディスプレイ2408に表示される。これらの制御や処理はICチップ質問機処理

部2526で行われる。ICチップから読み込まれた情報は、必要ならば、ICチップ情報格納部2530に格納される。携帯電話モードが選択されると、スイッチ部2514は、携帯用アンテナ部2502、入出力部2506、携帯電話機能処理部2524を接続し、ICチップ質問機兼用携帯電話は、通常の携帯電話としての機能を果たす。

### 【0053】

携帯電話モードのアプリケーションとして、ICチップから読み取った情報を使いたい場合は、前もってICチップから読み取った情報を格納しているICチップ情報格納部2530から情報を取り出し、使うことができる。このような応用例としては、ICチップを保険証明書として使い、医療サービス機関がICチップ質問機兼用携帯電話を使用する場合などが考えられる。ICチップ付き保険証明書の正当性をオフラインで確認できる場合は、ICチップ質問機モードで正当性を確認すればよく、携帯電話モードを使う必要がない。しかし、保険証が盗難に遭っている可能性が危惧されるような場合は、携帯電話モードに切り替えて、センターに該当ICチップ付き保険証明書が盗難に遭っていないかどうかを確認するような使い方をすることができる。このとき、例えば特定のキー操作を行うことによって、ICチップ質問機モードにて読み込みICチップ情報格納部2530に格納したICチップ情報をセンターに自動的に送信して問い合わせを行い、確認結果を直ちに受信して表示するようなアプリケーションを組み込んでおくと便利である。また、ICチップ質問機兼用携帯電話は、サービス機関に限らずICチップ利用者にとっても利便性が高い装置である。たとえば、利用者がICチップ付き保険証明書のICチップ内情報をもとに自分の加入している保険のサービス内容をセンターに自動問い合わせしたり、ICチップを証明書として使ってオンラインでサービスを受けたりすることが可能となる。この際にも、特定のキー操作などによって、ICチップ情報をICチップ質問機モードにて読み込みICチップ情報格納部2530に格納したその情報をセンターあるいはサービス実施機関に自動的に送信し、問い合わせを行って受信した結果を表示したり、所望のサービス実施機関に自動的に接続してICチップ情報を送信し、そのままサービスを受けるモードに移行できるようなアプリケーションを組み込んでお

くと便利である。

#### 【0054】

さらに、ICチップへの書き込みが必要な場合には、書き込むべき情報を最初にICチップ情報格納部2530に格納し、その後ICチップ質問機モードに切り替え、ICチップ情報格納部2530に格納されている情報をICチップに書き込むことで実行することができる。本実施例のように携帯電話にICチップ質問機能を付加することは、アンテナ2404やキー2410、ディスプレイ2408を兼用でき、ICチップ質問機を安価に実現できる利点がある。さらに、ICチップの応用として、ICチップ質問機モードと携帯電話モードを組み合わせ、それらのモードの間で情報を共有することにより、証明用ICチップの適用範囲を広げ、利便性を高めることができる。

#### 【0055】

ICチップ質問機と携帯電話を兼用にすることでサービスを提供するサービス実施機関側が享受できるメリットについて、医療保険証にICチップを使った医療保険を例にして説明する。医療サービス実施機関では、ICチップ質問機モードでICチップ所持者のICチップに保険証番号や利用者情報、医療受診情報を取り出すコマンドを送り、利用者情報や医療受診情報をICチップから取り出し、質問機の画面に表示させる。利用者情報に問題が合った場合、携帯電話モードにして、センターに保険証が盗難に遭っていないかの確認を行うこともできる。ICチップ質問機モードから携帯電話モードに簡単に切りかえられることおよび、ICチップ情報格納部が両方のモードで使えるため、利用者情報の入れ直しなどが不要となり、効率的な問い合わせが可能となる。また、ICチップのメモリに医療受診情報を入れておき、その情報を見ることにより、他の受診歴がないかの確認等も行うことができる。これは、投与薬の組み合わせによる副作用の危険性を防ぐ場合などに利用することができる。受診後、ICチップ質問機モードでICチップに格納されている医療受診情報に処置内容を記録させることもできる。

#### 【0056】

ICチップ付き証明書の正当性を確認するために、ICチップ内の情報と証明

書の表面に印刷されている情報を使って、正当性に対する信頼性を向上させる例について先に説明した。この場合、ICチップ内の情報と証明書の表面に記載されている情報を同時に読むことができる質問機があれば、正当性の確認の手間を省くことができ、利便性を高めることができる。文字情報読み取り兼用ICチップ質問機の実施例を図26に示す。ICチップ内の情報はアンテナ2602を介した通信で読み取り、証明書の表面の文字情報は文字情報読み取部2604で読み取る。文字情報読み取部2604は、文字を光学的に読み取るスキャナと光学的に読み取った文字をコードに変換する文字認識部からなる。このようにすることにより、例えば図18に示すようなICチップ付き証明書1802に添付されたICチップ1810内の情報と証明書表面の文字情報1808や1804を同時に読み取ることができる。なお、印刷情報として文字の代わりにバーコードが使用されている場合でも、同様に読み取り部2604で読み取ることができる。

#### 【0057】

文字情報読み取り兼用ICチップ質問機2608では、ICチップ内の情報と証明書の表面に印刷された文字等の印刷情報を読み取るだけではなく、それらの情報を使って、証明書の正当性の確認処理を行うことが可能である。処理手順を図27のフローチャートに示す。まず、文字情報読み取部2604にて証明書表面に印刷されている文字を読み取り(2704)、読み取った文字を認識する(2705)。その後、ICチップ質問機としての機能でアンテナ2604を介してICチップ内の情報を読み取る(2708)。次に、文字情報読み取部2604で読み取った内容とICチップ内の情報を使って正当性の確認を行い(2710)、正当性か否かの判定を行う(2712)。正当であれば、正当であることの表示(2714)、正当でなければ、正当でないことの表示を表示部2606に行う(2718)。正当性確認のための具体的処理内容は証明書のタイプに依存するが、その一つとして、ICチップの内容と文字として読み取った内容を照合してその一致を判定するという方法がある。さらに、正当性判定の確度を高める方法として、先に述べた“ICチップ情報と証明書記載情報を用いた正当性確認方法”がある。

#### 【0058】

ここでは、証明書の表面に印刷されているデジタルサインの情報を使う例について説明する。図18の例では、紙面に表示されている文字1808がデジタルサインの情報である。文字1808は、次式(8)の計算で求められたyの値を示すものである。

$$y = (x_1 + x_2)^{\star\star d} \bmod n \quad (8)$$

【0059】

上式において、dとnは証明書を発行している機関の秘密鍵である。yの計算には外部に漏らしてはいけない秘密鍵を使うので、yの計算は、安全な場所で行われ、その結果が証明書に印刷される。x1はICチップ内の情報であり、x2は証明書の表面に印刷されている重要な情報である金額(図18の例では1000)である。yが読み取られた後、文字情報読取兼用ICチップ質問機2608では、次式(9)の計算を行う。

$$z = y^{\star\star e} \bmod n \quad (9)$$

【0060】

得られたzは、式(8)の $(x_1 + x_2)$ に対応し、ICチップ内の情報と金額情報である。次に、ICチップの内容を読み込み、zからICチップの情報を引く。その結果、金額情報 $\times 2$ が得られる。

$$x_2 = z - x_1 \quad (10)$$

【0061】

数値 $x_2$ が、証明書の表面に書かれている金額情報と同一であれば、証明書1802の正当性が確認される。同一を確かめる方法としては、文字情報読取兼用ICチップ質問機2608のディスプレイ2606に表示されている数値と、証明書の表面に書かれている金額情報を目視で確認する方法も一つの方法である。

【0062】

上述のようにICチップを証明書につけることにより、証明書の正当性確認をICチップだけで行い、印刷技術による偽造防止対策があまり取られていない証明書の偽造の可能性を大幅に低減することができる。このようなICチップ付き証明書は、簡単な保険や切符のようなものに使うことができる。たとえば、旅行用の簡単な傷害保険をコンビニエンス・ストアなどで発行してもらおうとすると

、コンビニエンス・ストアではその場で発行する保険証に高度な印刷技術を適用できない場合があり、印刷技術だけでは偽造防止対策が万全でない可能性がある。このような場合、ICチップを使うことにより、偽造を困難にすることができる。簡単にICチップ付き証明書を発行する装置の実施例を図28に示す。

#### 【0063】

図28は、本発明の実施例による簡易型証明書発行装置の一例の概略図である。簡易型証明書発行装置2814は、一部証明書の内容が印刷されていない枚葉紙あるいはロール紙として用意された多数のICチップ付き証明書を証明書用紙格納部に格納し、証明書の発行時に、用紙印刷部2808で必要な情報を証明書に印刷する。こうして作成された証明書2802は、ICチップ2804が組み込まれているため、印刷技術だけで偽造することはできず、偽造を困難にしている。印刷などに使用する情報は、キー2812から入力する。

#### 【0064】

発行するICチップ付き証明書の偽造をより困難にするには、いくつかの方法がある。一つは、書き込み可能なICチップを使い、簡易型証明書発行装置2814で印刷した内容をICチップ内の情報として格納する方法である。書き込み可能なチップとして、一度しか書き込めないものを選べば、暗号鍵を使わずに書き込むことができる。複数回以上書き込み可能なチップであれば、暗号鍵を使って書き込む情報を不正に変更されないようにする必要がある。ICチップへの書き込みは、印刷時に、ICチップ書き込み部2806で行う。証明書の正当性を確認する際、表面に印刷されている情報とICチップに書かれている情報の照合を行い、同一であれば、正当な証明書とみなす。

#### 【0065】

別な方法として、ICチップ内の情報と印刷する情報を組み合わせる方法がある。これは、図19や図22で示したICチップ付き証明書を簡易型証明書発行装置2814で発行する方法である。ICチップ内の情報あるいは証明書の重要な情報と組み合わせた“ICチップ情報と証明書記載情報を使った正当性確認方法”を使い、簡易型証明書発行装置2814内で、そのデジタルサインを生成し、証明書に印刷する方法である。秘密鍵を簡易型証明書発行装置2814に格納

することが危険であれば、簡易型証明書発行装置2814をオンラインで証明書発行機関（サービス機関）につなぎ、ICチップ内の情報あるいは証明書の重要な情報を送り、証明書発行機関でデジタルサインを計算して簡易型証明書発行装置2814に送り返し、簡易型証明書発行装置2814では送付されてきたデジタルサインを印刷するようにしてもよい。

#### 【0066】

証明書を使ったサービスには、生命保険をはじめ傷害保険、健康保険（医療保険）、商品券、株券、紙幣、映画のチケット、切符など、さまざまなものがある。証明書を用いたサービスの一般的な流れは図29のようになる。サービス機関2902が証明書2904を発行し、それを利用者2910が受け取る（2906）。利用者はサービス機関に代償、たとえば、お金などを支払う場合がある。証明書を手にした利用者2910はサービスを受けたい場合、サービス実施機関2914に証明書2904を提示、あるいは譲渡し（2912）、サービスを受ける（2916）。サービスには、サービス機関2902とサービス実施機関2914とが同一な場合もあるし、そうでない場合もある。たとえば、サービス機関とサービス実施機関が異なるサービスの例として健康保険がある。健康保険のサービス機関は健康保険組合であり、それらが保険証を発行しているが、健康保険のサービスは病院等のサービス実施機関で受ける。サービス機関とサービス実施機関が異なる場合は、その二者間で何らかの代償が払われていることが多い。一方、切符などを使った交通機関による移動サービスは、サービス機関とサービス実施機関が同一なサービスの例である。

#### 【0067】

証明書を使ったサービスでは、証明書の正当性を前提として、サービス機関2902、利用者2910、サービス実施機関2914からなるサービスシステムが安全に働くことができる。しかし、証明書が偽造されるような可能性がある場合、証明書以外の別な方法で利用者の確認を行う必要がありシステム運営コストの上昇をまねくことになり、極端な場合にはサービスシステムそのものが破綻してしまうことも考えられる。本発明の実施例によるICチップ付き証明書は、証明書の偽造をより困難にするため、偽造によってサービスシステムが破綻を来す

ことを回避したり、システム全体の運営コストを下げるよう作用するものである。

### 【0068】

本発明の実施例のICチップ付き証明書を使ったサービスシステムの実施例を図30に示す。サービス機関3002から利用者3010には、従来の証明書2904の代わりに、ICチップが装着されたICチップ付き証明書3004を発行する(3006)。利用者3010はサービスを受ける場合、サービス実施機関3014にICチップ付き証明書3004を提示、あるいは譲渡することにより(3012)、サービスを受け取る(3016)。サービス実施機関3014では、図24に示したICチップ質問機兼用携帯電話2406や図26に示した文字情報読み取り兼用ICチップ質問機2608を使ってICチップ内の情報を読み取り、ICチップ付き証明書の正当性の確認を行ったり、ICチップ内の情報と証明書の表面に印刷されている情報を使ってICチップ付き証明書の正当性の確認を行うことができる。ICチップ付き証明書3004を使うことにより、印刷技術で偽造対策を図った従来の証明書2904に比べて、偽造が困難になり、偽造によるサービスシステムの破綻の可能性を減らしたり、システム運営のコストを下げることができる。ICチップ付き証明書の配布方法としては、図22に示したはがき2202を使って配布する方法もある。ICチップ内の情報としては、ICチップ毎に異なるICチップ番号、あるいは発行者を示すような同じIC番号であるICチップ番号が必須である。それ以外に、利用者情報や利用状況などの付随情報を記録するフィールドがあってもよい。サービス機関に関する情報を記録する場合もある。どのような付随情報を持つかは、サービスの種類あるいはサービスの内容に大きく依存する。さらに、既に述べたICチップ内の情報と証明書に印刷されている情報との照合、あるいは“ICチップ情報と証明書記載情報を使った正当性確認方法”などの方法で正当性の確認を行うことができる。

### 【0069】

ICチップ付き証明書を直接使う代わりに、ICチップ付きシールを使ってサービスを受け取ることもできる。ICチップ付きシールを使ったサービスシステムの実施例を図31に示す。サービス機関3102は、利用者3112にICチ

ップ付きシール3108を配布する（3106）。配布方法は、例えば図23に示すようにして証明書3104にICチップ付きシール3108を直接貼っておき、証明書3104を送ると同時にICチップ付きシール3108を配布する方法がある。ICチップ付きシールだけでサービスを受ける場合は、証明書からICチップ付きシールをはがして使用する方法も考えられる。また、ICチップ付き証明書以外にICチップ付きシールも配布し、ICチップ付きシールだけで使用する方法が考えられる。別な方法として、図21に示すはがきを使って、ICチップ付きシール3108を配布する方法もある。ICチップ付きシール3108を受け取った利用者3112は、それをICチップ付きシールの台紙3110などに貼り、サービス実施機関3116に提示することにより（3114），サービスを受けることができる（3118）。

#### 【0070】

ICチップ付きシールを用いたサービスシステムが普及すると、利用者は複数のICチップ付きシールを所有することになる。規格化された台紙があると利用者の利便性が増す。台紙の実施例を図32に示す。まず、ICチップ付きシール3204の大きさを規格化したもの想定する。台紙3202は、シールを貼りやすく、規格化されたシールの大きさにあった窓み3206や3208をつけ、シールを貼りやすく、かつはがれにくくしたものである。

#### 【0071】

また、ICチップ付きシールやICチップ付き証明書を持ち運ぶことが多くなると、ICチップの情報を読み取られないような対策が必要になる。ICチップ付きシールやICチップ付き証明書は、一般に、定期入れ等のカードケースに入れて、胸ポケット等に入れられている場合が想定される。混んだ電車内等では、胸ポケットに強力な質問機をあてられて、胸ポケットに入っているICチップの内容を読まれてしまう危険がある。これを回避するためのカードケースの実施例を図33に示す。図33はカードケースを開いた状態を示している。このカードケース3302は、内側にアルミなどの金属膜3304や3306を組み込み、外部からの電磁波や電波を遮断する機能を持つ。カードケース3302に入れられているICチップ付きシール3204などは、金属膜3304、3306が電

磁波や電波を通さないため、不正な読み込みや書き込みを防止することができる。

#### 【0072】

ICチップ付き証明書の正当性の確認精度をさらに上げる方法として、サービスを実施する時にサービス機関にICチップ情報を確認する方法がある。そのようなサービスシステムのシステム例を図34に示す。まず全体の流れを説明する。サービス実施機関3428が利用者3422にサービスを実施する際(3424)、ICチップ付きシールあるいはICチップ付き証明書3430の提示や譲渡を求める(3426)。サービス実施機関3428は、ICチップ内の情報あるいはシールや証明書に記載されている情報をサービス機関3402の利用権情報確認センター3406に送り、正当性の問い合わせを行う(3418)。利用権情報確認センター3406には、あらかじめ、ICチップを使った利用権に関する情報3502(図35)がサービス機関内のサービス部門3404から転送されている(3408)。

#### 【0073】

なお、図34に図示したサービス機関3402、サービス機関3402のサービス部門3404や利用権情報確認センター3406、サービス実施機関3428等はそれぞれコンピュータシステムを備え、それらのコンピュータシステムは専用回線、公衆回線あるいはインターネット等により相互に接続されている。ただし、サービス実施機関3428に関しては、コンピュータシステムを備えずにICチップ質問機兼用携帯電話等のみを備え、ICチップ質問機兼用携帯電話等から公衆回線を介してサービス機関3402と接続して情報のやり取りを行うシステム構成であってもよい。図34に破線で示した矢印は物やサービスの提供関係を表し、実線の矢印は前記各機関やセンターに設置されたコンピュータ間における通信文やデータの流れを表している。破線の矢印と実線の矢印の意味は、サービスシステムのシステム構成を示す以下の図においても同様である。

#### 【0074】

利用権情報確認センター3406のサーバに格納・管理する情報3502の例としては、図35で示すようにICチップ番号3504と、利用者情報3506

、サービスの内容3510がある。また、正当性を確認するための情報3508もサービス部門3404から利用権情報確認センター3406に送られている。正当性を確認するための情報3508には、ICチップ情報とシールや証明書に記載されている情報を組み合わせて正当性を確認する方法や情報が記載されている。正当性の確認方法には、以下のようないくつかの方法が考えられる。

#### 【0075】

##### (1) ICチップ登録確認方法

ICチップ番号3504を使い、サービス実施機関3428から送られてきたICチップ番号が登録されているかを確認することにより正当性を確認する方法である。

#### 【0076】

##### (2) ICチップ登録および有効性確認方法

ICチップ番号3504を使い、サービス機関から送られてきたICチップ番号が登録されているかを確認し、更にそれが使用された時期が有効期間3514内か否かを確認し、正当性を確認する方法である。

#### 【0077】

##### (3) ICチップ登録および利用状況確認方法

ICチップ番号3504を使い、サービス機関から送られてきたICチップ番号が登録されているかを確認し、更に利用状況3514の情報を使って正当性を確認する方法である。証明書が商品券やチケットであるような場合、一度使われると利用状況3514に使用済みのフラグを立て、使用済みのフラグが立っているICチップ番号についてサービス実施機関から問い合わせがあった場合、二重使用であると判断して不正使用と判定する方法である。

#### 【0078】

##### (4) ICチップ登録と表面に印刷された情報による確認方法

これは、既に述べた“ICチップ情報と証明書記載情報を使った正当性確認方法”である。正当性確認情報3508には、デジタルサインを検証するための公開鍵が登録されている。

#### 【0079】

利用権情報確認センター3406では、正当性を確認するための情報3508に基づいて、サービス実施機関3428から正当性の問い合わせに付随して送られてきた情報を使って正当性の判定を行う。サービス実施機関3428から送られてくる情報は、そのサービスシステムが採用している正当性確認方法に依存するが、ICチップ番号は必須である。利用権情報確認センター3406では、サービス実施機関3428からの問い合わせ情報などの利用状況3512をサービス部門3404に報告する（3410）ことができる。

#### 【0080】

利用権情報確認センター3406に設けられたコンピュータシステムの有する機能の一例を図36に示す。サービス部門やサービス実施機関からの問い合わせは、送受信部3604が受け、利用権情報格納部3608に格納された利用権情報3502を使って処理部3606で処理を行う。

#### 【0081】

正当性判定の簡単な方法の一つは、前記（1）に述べたICチップ登録確認方法であり、ICチップ内の情報が利用権情報確認センター3406のICチップ情報格納部3608に登録されたICチップ情報3504とサービス実施機関3428から送られてきたICチップ情報が同じ内容かであるか否かを確認する方法である。一致すれば正当と認め、そうでなければ正当でないと判定する。

#### 【0082】

さらに、正当性判定の信頼性を向上させる方法は、既に述べた”ICチップ情報と証明書記載情報を使った正当性確認方法”を使って、ICチップ情報とシールあるいは証明書の表面に記載されている情報とを組み合わせて正当性を確認する方法である。公開鍵暗号方式を利用する場合、利用権情報3502には正当性確認情報3508として公開鍵が格納される。サービス実施機関から送られてきたICチップ情報を公開鍵で復号化し、証明書の記載情報と照合することにより正当性を確認することができる。この場合は、ICチップとそれが装着されているシールや証明書との対応も確認できる。

#### 【0083】

サービス実施機関3428における正当性確認処理手順の一例を図37に示す

。サービス実施機関は、利用者からICチップ付き証明書あるいはICチップ付きシールの提示を受けると、前述の質問機を用いてICチップの内容を読み取り（3704），必要ならば表面の文字情報を読み取り（3706），それらの情報を利用権情報センター3406に送り，正当性の問い合わせを行う。利用権情報センターから正当性の結果を受け取り（3710），正当であることが確認できれば，サービスを実施する（3714）。一方，正当であることが確認できなければ，サービスを拒否する（3718）。

#### 【0084】

利用権情報確認センター3406の処理部3606で行う正当性の確認の処理手順の一例を図38に示す。サービス実施機関3428からの正当性の確認要求を受けると（3804），利用権情報格納部3608に格納されている利用権情報3502（図35参照）から，確認要求と一緒に送られてきたICチップ番号を検索する（3806）。該当ICチップがなければ，正当性が確認できなかつたという結果を返す（3820）。該当チップがあれば，正当性確認情報3508に書かれている確認方法と確認のために使う情報とを使って正当性を確認する（3810）。確認できれば，利用情報3512を更新し（3814），正当であるという結果をサービス実施機関3428に返す（3816）。一方，正当性を確認できなければ，正当性が確認できなかつたという結果をサービス実施機関3428に返す（3820）。

#### 【0085】

ICチップ付きシールやICチップ付き証明書が普及すると，ICチップの情報を照合する利用権情報確認センターの処理を代行するサービス機関代行センターを設置するのが便利である。サービス機関代行センターを含ませたサービスシステムにおける各機関の関係例を図39に示す。サービス機関代行センター3906は，一つ以上のサービス機関3902（図には一つのサービス機関のみを示す）の利用権情報確認センター3406の機能を代行するものである。サービス機関3902は，ICチップ付きのシールあるいはICチップ付きの証明書3910を利用者3922に配布する（3912）。それに並行して，サービス機関3902は，サービス機関代行センター3906に利用権に関する情報を送る（

3904)。利用者3922は、サービスを受けようとするサービス実施機関3928にICチップ付きのシールあるいはICチップ付きの証明書3930を提示あるいは譲渡する(3926)。サービス実施機関3928は、ICチップ付きシールあるいはICチップ付き証明書3930の正当性を確認するために、サービス機関3902ではなくサービス機関代行センター3906に正当性の問い合わせを行う(3918)。サービス機関代行センター3906は、サービス実施機関から送られてきた情報を用いて正当性の確認処理を行い、その結果をサービス実施機関に返す(3920)。サービス実施機関3928は、ICチップ付きのシールあるいはICチップ付きの証明書3930が正当であれば、サービスを提供する(3924)。

#### 【0086】

複数のサービス機関による複数のサービスシステムが併設され利用者が多種類のICチップ付き証明書を所持しているような状況を想定すると、サービス機関代行センター3906を設置することでサービス実施機関3928での正当性確認処理の手続が簡素化される。証明書の正当性の問い合わせをするとき、サービス実施機関はICチップ付き証明書を発行した個々のサービス機関を意識することなく常に同じサービス機関代行センター3906に問い合わせを行えばよくなるからである。また、利用者が所持する複数のICチップ付き証明書にかかる複数のサービスの利用権情報をサービス機関代行センター3906で一括管理できるため、いずれかのサービス実施機関においてある利用者のあるサービスに関するICチップ付き証明書が不正使用されたとの情報を取得したとき、それ以後その利用者に対するサービスを全て拒否するような迅速な対応が可能になる。これは例えば、1枚の台紙に貼った複数のICチップ付き証明書が盗難にあったような場合、被害を最小限に抑えるのに有効である。

#### 【0087】

サービス機関代行センター3906は、サービス実施機関3928からの正当性の確認の問い合わせ以外にサービスの内容に関する問い合わせに対しても回答することが可能である。たとえば、利用者に設定(登録)されているサービスの具体的な内容やサービスのレベルなどの情報に対する問い合わせに対して回答する

ことができる。そのためには、あらかじめ、サービス機関からサービス機関代行センターにサービスの内容に関する情報を送っておく必要がある。

#### 【0088】

また、サービス機関代行センター3906は、利用者3922からのサービス内容等に関する問い合わせ（3914）に対して、その回答を利用者3922に返すことができる（3916）。誰もが勝手に問い合わせができないようにするために、これらの問い合わせが本人からのものであるかどうかの確認をICチップの番号で行うことができる。サービス機関代行センター3906への問い合わせには、図24に示したようなICチップ質問機兼用携帯電話を用いることができる。サービスに関する問い合わせを携帯電話等で簡単に行うことができるようになるには、図40に示すように、ICチップのメモリ4002中にICチップ番号4004以外にサービス機関の識別子4008やサービス機関代行センターの問い合わせ先の電話番号4010を格納しておけばよい。ICチップ質問機モードでICチップ2402にICチップ質問機兼用携帯電話2404をかざし、ICチップに問い合わせコマンドを送り、ICチップ番号、サービス機関識別子、問い合わせ先電話番号をICチップから読み込む。

#### 【0089】

図41にICチップ質問機兼用携帯電話の表示画面4102の例を示す。ICチップ質問機モードに切り替えられたICチップ質問機兼用携帯電話は、ICチップの情報を読み取り、読み取った情報はICチップ情報格納部2530に格納する。読み取ったサービス機関の内容等の情報は、ICチップ質問機モード情報欄4104にも表示される。ICチップ内の情報を読み取った後、携帯電話モードに切り替え、サービスの問い合わせを選ぶと、ICチップ情報格納部2530に格納された問い合わせ先電話番号等の情報を用いてサービス機関代行センターへ自動的に問い合わせが行われ、その結果が携帯電話モード情報欄4106に表示される。

#### 【0090】

サービス機関代行センター3906は複数のサービス機関の利用権情報の確認を行うために、図42に示すように、サービス機関ごとの利用権情報4202、

4214, …を保管・管理する。ICチップ番号4204(4216)から始まる一つのレコードはICチップ一つに対応し、サービス機関から送られてきたデータである。ICチップ番号4204(4216)は、サービス機関がサービスを行うICチップの識別コードである。すなわち、利用権情報4202, 4214にICチップ番号が登録されているということは、多くの場合、そのICチップ番号をもつICチップがサービスを受けるために有効であることを示している。利用者情報4206(4218)は、利用者に関する情報であり、氏名などの情報である。どのような情報をサービス機関代行センターに渡すかは、各々のサービス機関のサービスやポリシーに依存する。正当性確認情報4208(4220)は、ICチップ情報とシールや証明書に記載されている情報を組み合わせて正当性を確認する方法や確認に際して使用される情報が記載されている。たとえば、公開鍵暗号方式を使うのであれば、その公開鍵が格納されている。サービス内容4210(4222)は、サービス実施機関3928や利用者3922にサービス内容を伝えるために使われる。利用状況4212(4224)は、サービス実施機関3928が、正当性を確認した後、ICチップ付きのシールあるいはICチップ付きの証明書の利用状況を格納するためのフィールドである。たとえば、商品券などであれば、商品券をあらわすICチップ付きの証明書は、使用されたということを利用状況に記録する。これは、商品券が2度使われたことを検知するものである。ICチップ付きの証明書である商品券が使われた際は、正当性確認以外に利用状況の確認も必要である。利用状況4212でどのような情報を記録・確認し、どのようなアクションを起こすかは、サービス機関3902のサービス内容やポリシーに依存する。

#### 【0091】

サービス機関代行センター3906に設置されたコンピュータシステムの構成は、基本的には、図36に示した利用権情報確認センターのコンピュータシステムの構成と同じである。利用権情報格納部3608には、サービス機関Aの利用権情報4202やサービス機関Bの利用権情報4214が格納されている。処理部3608では、サービス機関や利用者、サービス実施機関から送られてきた指示を利用権情報格納部3608の情報を使って処理を行う。

## 【0092】

サービス機関代行センター3906での正当性の確認処理方法は、利用権情報確認センター3406での処理内容とほとんど同じである。図43を用いて処理の例を説明する。サービス機関代行センター3906では、サービス実施機関3928からの正当性の問い合わせを受信すると(4304)，問い合わせ情報の中から、サービス機関識別子を取り出す(4306)。次に、利用権情報格納部3608の中にある各サービス機関の利用権情報4202や4214の中から該当するサービス機関の利用権情報を選ぶ(4308)。該当利用権情報から確認要求と一緒に送られてきたICチップ番号を検索する(4310)。該当ICチップが登録されていなければ、正当性が確認できなかったという結果を返す(4324)。該当チップがあれば、正当性確認情報4208あるいは4220に書かれている確認方法と確認のために使う情報を使って正当性を確認する(4314)。確認できれば、利用情報4212あるいは4224を更新し(4318)，正当性であるという結果をサービス実施機関3928に返す(4320)。一方、正当性を確認できなければ、正当性が確認できなかったという結果をサービス実施機関3928に返す(4324)。

## 【0093】

サービス機関代行センター3906での利用者3922からの問い合わせ(3914)に対する処理の例を図44に示す。利用者からのサービスに関する問い合わせに対する処理も、図43で示した正当性の問い合わせに関する処理と同じような処理手順となる。利用者からサービスに関する問い合わせを受信すると(4404)，問い合わせ情報の中から、サービス機関識別子を取り出す(4406)。次に、利用権情報格納部3608の中にある各サービス機関の利用権情報4202や4214の中から該当するサービス機関の利用権情報を選ぶ(4408)。該当利用権情報から問い合わせ情報と一緒に送られてきたICチップ番号を検索する(4410)。該当ICチップが登録されていなければ、サービス内容を返せないという結果を返す(4424)。該当チップがあれば、正当性確認情報4208あるいは4220に書かれている確認方法と確認のために使う情報を使って正当性を確認する(4414)。確認できれば、サービス内容4210

あるいは4222を取り出し(4418), サービス内容を利用者3922に返す(4420)。一方、正当性を確認できなければ、サービス内容を返せないという結果を返す(4424)。サービス内容の問い合わせに関する正当性の確認は、サービスの実施に関する正当性の確認より厳密性が必要とされない場合がある。どのような正当性の確認を行うかは、サービスに依存している。

#### 【0094】

サービス機関代行センターが、複数のサービス機関が発行したICチップのICチップ番号で、ICチップ付き証明書やシールの正当性を確認する場合、各ICチップのICチップ番号を唯一無二にする必要がある。唯一無二にしなければ、同じICチップ番号が使われる可能性があり、サービス機関代行センターで正当性の確認や管理面で混乱を来す可能性がある。これは、サービス機関代行センターを使わず、サービス機関が独自にICチップ番号を使って、正当性を確認する場合も起こり得る。このような問題を解決するためにICチップ番号を唯一無二にするように管理する必要がある。唯一無二のICチップ番号を持つように管理されたICチップをユニーク番号付きICチップと呼ぶ。また、サービス機関がユニーク番号付きICチップを使わないで、サービス機関が発行するICチップのICチップ番号にサービス機関の識別子として同一のICチップ番号を使った場合は、複数のサービス機関がそれぞれ独自に識別子をつけるため、同じICチップ番号となってしまう可能性があり、正当性の確認や管理面で混乱を来す可能性がある。チップごとに唯一無二のICチップ番号やあるいはサービス機関ごとに異なったICチップ番号を管理し、番号を与えるセンターが必要となる。そのようなセンターをICチップ発行センターと呼ぶ。このセンターは、ICチップの製造メーカーでも、メーカー以外の組織でもよい。

#### 【0095】

ICチップ発行センターとサービス機関の間の関係を図45に示す。ICチップ発行センター4502は、それぞれのサービス機関4516, 4518の要求(4504, 4510)に従い、ICチップが組み込まれたICタグ付きシール4508や4514を配布する(4506, 4512)。ICチップの中のICチップ番号は、ICチップ発行センター4502がユニークな番号を振って、そ

それぞれのサービス機関に配布する。

#### 【0096】

ユニークな番号の振り方の例として、以下の方法がある。

(1) サービス機関が取得した物品番号（日本では、JANコード（Japan Art ICle Number：日本物品番号））とそれぞれのシーケンシャル番号を与える方法。

(2) ICチップに連続した、あるいは唯一無二の番号を当て、それらを必要に応じてサービス機関に配布する方法。

#### 【0097】

ここで（1）の方法は、物品番号を使うため、物品番号の部分を読めば、どこ のサービス機関のものかが容易に分かる特徴がある。（2）の方法は、JANコードなどを使わなくてもICチップを生成できる利点がある。ただし、それぞれのサービス機関では、ばらばらのICチップ番号を管理する必要が出てくる。サービス機関のみを種別する場合は、物品番号などを利用するのが一つの方法である。

#### 【0098】

ICチップ発行センター4502がユニークな番号を振るために、管理するICチップ番号とサービス機関の対応表の例を図46に示す。前記（1）の場合でも（2）の場合でも、ICチップ発行センター4502が管理しているテーブル4602の形式は図46に示す通りである。（1）の方法では、テーブル4602において、ICチップ番号4604として物品番号を割り当てられたICチップは、その物品番号を利用するサービス機関4606で利用されることを示す。この場合には同じICチップ番号を持つICチップが複数個あることになるが、それらは同じサービス機関に割り当てられる。一方、（2）の方法では、ひとつ一つのICチップはそれぞれユニークなICチップ番号4604をもち、それぞれのICチップは、どれか一つのサービス機関4606に割り当てられている。

#### 【0099】

サービス機関代行センターが存在する場合の、ICチップ発行センターとサービス機関及びサービス機関代行センターの間の関係を図47に示す。サービス機

関代行センター4728は、ICチップ番号に不審なものがあれば、ICチップ発行センター4702に問い合わせ(4720)，その結果を知ることができる(4722)。たとえば、そのICチップ番号が、万が一、ICチップ発行センター4702で発行された番号でなければ、ICチップが偽造された可能性があることを知ることができる。ICチップの偽造は半導体工場で行う必要があるため、印刷技術による偽造に比べて極めて困難である。しかし、何らかの手段で半導体工場を使うことができれば、偽造することが全く不可能というわけでもない。ICチップ発行センター4702があれば、ICチップの番号を一元的に管理しているため、万が一、偽造が起こっても発見や対策が容易になる。

#### 【0100】

本発明の実施例によれば、証明書にICチップを添付することにより、証明書の正当性を印刷技術だけではなくICチップを使って確認できるため、証明書の偽造を困難にすることができる、サービス機関やサービス実施機関が行うサービスシステムの信頼性を向上することができる。証明書の代わりに小型のICチップ付きシールを携帯することにより、利用者が証明書を所有する頻度が増えて必要な時にサービスを受けることができるようになり、利用者の利便性が増す。さらに、サービス実施機関で利用者がサービスを受けるたびに、サービス実施機関がサービス機関内の利用権情報確認センターにICチップ付きシールやICチップ付き証明書の正当性の確認を問い合わせることにより、正当性の確認の信頼度を向上させることができる。さらに、利用権情報確認センターの機能を代行するサービス機関代行センターを設けると、サービス機関がICチップ付きシールやICチップ付き証明書の正当性の確認をする必要がなくなる。

#### 【0101】

以下に、本発明の他の態様を列挙する。

1. 通信機または通信手段との間で無線通信を行うことによりその内部のメモリに記憶されたデータを無線送信するように構成されたICチップがその一の面に取り付けられるか又はその内部に配置されたシート状媒体の前記ICチップのメモリに記憶されたデータのうちの少なくとも一部は当該媒体を利用して当該媒体の所持者が一のサービスを受ける権利を有するサービス機関に関する第一の情報

、前記所持者の個人情報である第二の情報または当該ICチップを他と識別するユニークな第三の情報の少なくとも一つであり、前記第一乃至第三の情報のうち少なくとも一つの情報およびそれをキーとしたその関連情報を記憶手段に格納することにより複数個のICチップ情報を管理可能とし、前記ICチップ内の前記第一乃至第三の情報うちの少なくとも一つの情報を受信し、それをキーとして前記関連情報を前記記憶手段から読み出し、前記受信情報と前記読み出し情報に基づいて当該媒体または当該媒体が有する証明事項が正当なものであるか否かの判定を行うシート状媒体の正当性判定方法。

#### 【0102】

2. 通信機または通信手段との間で無線通信を行うことによりその内部のメモリに記憶されたデータを無線送信するように構成されたICチップがその一面に取り付けられるか又はその内部に配置されたシート状媒体の前記ICチップのメモリに記憶されデータのうちの少なくとも一部は当該媒体を利用して当該媒体の所持者が一のサービスを受ける権利を有するサービス機関に関する第一の情報、前記所持者の個人情報である第二の情報または当該チップを他と識別するユニークな第三の情報の少なくとも一つであり、当該ICチップの所持者が前記一のサービスを受ける権利を有する場合には当該ICチップが有する前記第一乃至第三の情報のうちの少なくとも一つが前記権利を有するもののデータ集合として記憶手段に格納されており、前記ICチップ内の前記第一乃至第三の情報うちの少なくとも一つの情報を受信し、受信したデータと前記データ集合とを照合することを特徴とするシート状媒体のデータ照合方法。

#### 【0103】

3. 通信機または通信手段との間で無線通信を行うことによりその内部のメモリに記憶されたデータを無線送信するように構成されたICチップがその一面に取り付けられるか又はその内部に配置されたシート状媒体の前記ICチップのメモリに記憶されたデータのうちの少なくとも一部は当該ICチップに付与された識別データであり、当該媒体の所持者に当該媒体を利用してサービスを受ける権利が付与されている場合には当該媒体のICチップが有する前記識別データが前記権利を有するもののデータ集合として記憶手段に格納されており、前記ICチ

ップ内の前記識別データを受信し、受信したデータと前記データ集合とを照合することにより前記サービスを受ける権利を有するか否かの判定を行うことを特徴とするシート状媒体のデータ照合方法。

【0104】

4. 通信機または通信手段との間で無線通信を行うことによりその内部のメモリに記憶されたデータを無線送信するように構成されたICチップがその一面に取り付けられるか又はその内部に配置されたシート状媒体の前記ICチップのメモリに記憶されたデータのうちの少なくとも一部は当該ICチップに付与された識別データであり、当該媒体の所持者が当該媒体を利用してサービスを受ける権利を有する場合には当該媒体のICチップが有する前記識別データが前記権利を有するもののデータ集合として記憶手段に格納されるとともに、個々の前記識別データをキーとして当該サービスを受けることができる期限、当該サービスを受けることができる回数および当該サービスを受けることができる残回数の少なくとも一つがデータ集合として前記記憶手段に格納され、かつ、これらデータ集合は逐次更新されるように構成され、前記媒体のICチップ内の前記識別データを受信し、受信したデータと前記データ集合とを照合することにより前記サービスを受ける権利を有するか否かの判定を行うことを特徴とするシート状媒体のデータ照合方法。

【0105】

5. 通信機または通信手段との間で無線通信を行うことによりその内部のメモリに記憶されたデータを無線送信するように構成されたICチップがその一面に取り付けられるか又はその内部に配置されたシート状媒体の前記ICチップのメモリに記憶されたデータのうちの少なくとも一部は当該ICチップを他のICチップと識別するための固有データであり、当該媒体が市場に流通してその所持者が特定のサービスを受けるための標識機能を付与されている期間中、当該媒体のICチップの前記固有データまたは前記固有データをキーとしたデータが前記標識機能を有するもののデータ集合として記憶手段に格納されており、前記媒体のICチップ内の前記固有データを受信し、受信したデータと前記データ集合とを照合することにより前記サービスを受ける権利を有するか否かの判定を行うこと

を特徴とするシート状媒体のデータ照合方法。

【0106】

6. 前記シート状媒体は紙、プラスチック、シール付きフィルムのいずれか一であることを特徴とする前記2～5のいずれか1項記載のシート状媒体のデータ照合方法。

7. 前記シート状媒体は、生命保険証、傷害保険証、健康保険証、商品券、株券、紙幣、チケット、切符のいずれかの用途に使用されるものであることを特徴とする前記2～5のいずれか1項記載のシート状媒体のデータ照合方法。

【0107】

8. サービス実施機関からサービスを受ける権利を有することを証明する手段としてユニークな識別情報を格納したICチップを付属させたシート状媒体を発行するとともに、発行したICチップの識別番号と関連付けてサービス利用権に関する情報をサーバに格納しておき、前記サービス実施機関の端末から前記ICチップの識別情報をもとにした問い合わせを受信したとき前記サーバに登録されているICチップの識別情報あるいは当該識別情報に関する情報をもとに前記問い合わせに対する回答を生成し前記サービス実施機関の端末に送信することを特徴とするサービスシステム。

サービス利用権に関する情報には、ユーザ情報、正当性確認情報、サービス内容、利用状況、有効期限などの情報を含ませることができる。

【0108】

9. サービス実施機関からサービスを受ける権利を有することを証明する手段としてユニークな識別情報を格納したICチップを付属させたシート状媒体を発行するサービス機関と、前記サービス機関と通信回線で接続された情報センターとを含み、前記情報センターは、ICチップの識別番号と関連付けられたサービス利用権に関する情報を前記サービス機関から受信してサーバに格納しておき、前記サービス実施機関の端末からICチップに関して前記識別情報をもとにした問い合わせを受信したとき前記サーバに登録されているICチップの識別番号あるいは当該識別情報に関する情報をもとに前記問い合わせに対する回答を生成し前記サービス実施機関の端末に送信す

ることを特徴とするサービスシステム。

【0109】

前記サービスシステムにおいて、サーバは、正当性の確認方法に関する情報を保持し、当該情報に従って問い合わせに対する回答を生成し、サービス実施機関の端末に送信するようにしてもよい。

【0110】

本発明の別の態様による情報処理システムは、証明のために用いられたICチップに関する問い合わせを受信し、当該問い合わせに対する回答を返信するシステムであり、ICチップに関する問い合わせを受信し処理結果を返信する送受信部と、ICチップの識別情報をキーにして当該識別情報に付隨する情報を表形式で格納したICチップ情報格納部と、ICチップ情報格納部内の情報を検索して、問い合わせに対する結果を生成する処理部とを備える。問い合わせを行うのは、ICチップを付属させたシート状媒体あるいはICチップ付き証明書の提示を受けてサービスを提供するサービス実施機関の場合もあるし、利用者の場合もある。サービス実施機関からの問い合わせは通常、利用者から提示されたICチップあるいはICチップ付き証明書の正当性に関する問い合わせであり、利用者からの問い合わせとしてはサービス内容の問い合わせ等が考えられる。情報処理システムのICチップ情報格納部にICチップの正当性確認の方法に関する情報を格納しておき、処理部は送受信部で受信した問い合わせ情報をその正当性確認の方法に従って処理し、処理結果を送受信部から問い合わせ先に送信するようにしてもよい。

【0111】

本発明の他の態様によるサービスシステムは、サービスを管理するサービス機関を含み、サービス機関はサービスを実施するサービス実施機関からサービスを受ける権利を有することを証明する手段としてユーザにユニークな識別情報を格納したICチップを付属させたシート状媒体を発行するとともに発行したICチップの識別番号と関連付けてサービス利用権に関する情報を表形式にしてサーバに格納しておき、サーバはユーザの端末からICチップの識別情報をもとにサービスに関する問い合わせを受信したとき当該識別情報に関連して登録されている

サービス利用権に関する情報をもとに問い合わせに対する回答を生成し前記ユーザの端末に送信することを特徴とする。

【0112】

本発明の他の態様によるサービスシステムは、サービスを管理するサービス機関と通信回線で接続された情報センターを含み、情報センターは、サービスを実施するサービス実施機関からサービスを受ける権利を有することを証明する手段としてユーザにユニークな識別情報を格納したICチップを付属させたシート状媒体を発行したサービス機関から、発行されたICチップの識別番号と関連付けてびサービス利用権に関する情報を表形式にしたデータを受信してサーバに格納しておき、サーバはユーザの端末からICチップの識別情報をもとにサービスに関する問い合わせを受信したとき当該識別情報に関連して登録されているサービス利用権に関する情報をもとに問い合わせに対する回答を生成しユーザの端末に送信することを特徴とする。

【0113】

本発明の他の態様による質問機は、無線通信を行う通信処理部と、証明のために用いられたICチップ内の情報を非接触で読み取るICチップ読み取り処理部と、ICチップ読み取り処理部で読み取った内容を表示する表示部と、通信処理部とICチップ読み取り処理部の機能を選択するスイッチ部とを含むことを特徴とする。

【0114】

本発明の他の態様による質問機は、無線通信を行う通信処理部と、証明のために用いられたICチップ内の情報を非接触で読み取るICチップ読み取り処理部と、ICチップ読み取り処理部で読み取ったデータを格納するICチップ情報格納部と、通信処理部とICチップ読み取り処理部との機能を選択するスイッチ部とを含み、通信処理部での通信処理実行中にICチップデータ格納部に格納されたデータを送信する機能を有することを特徴とする。

【0115】

質問機は、証明書に印刷された文字やバーコード等の情報を読み取るスキャナを備えることができる。また、ICチップ内の情報およびスキャナで読み取った

印刷情報を比較し、証明書の正当性を判定する正当性判定処理部を備えることもできる。

【0116】

【発明の効果】

本発明によれば、例えば、セキュリティの高い証明書を提供できる。

【図面の簡単な説明】

【図1】

非接触ICチップの一例を示す概略構成図。

【図2】

ICチップをシールに装着したICチップ付きシールの一例を示す断面図。

【図3】

ICチップをシールに装着したICチップ付きシールの一例を示す平面図。

【図4】

ICチップをテープ状に装着した一例を示す構成図。

【図5】

パッド付き非接触ICチップの一例を示す構成図。

【図6】

パッド付き非接触ICチップを、テープ状に実装した外部アンテナと接続した一例を示す構成図。

【図7】

パッド付き非接ICチップの複数を、長いテープ状に実装した外部アンテナと接続したICチップ付きテープの一例を示す説明図。

【図8】

テープに上からかぶせる外部アンテナのみついているテープの一例を示す説明図。

【図9】

ICチップの反対側からも外部アンテナと接続したICチップ付きテープの一例を示す説明図。

【図10】

ICチップ付きテープを分断し、ICチップ付きタグとした例の説明図。

【図11】

印刷技術を使い導電性粒子を印刷して、ICチップの反対側からも外部アンテナと接続したICチップ付きテープの一例を示す構成図。

【図12】

テープに平行に二つの外部アンテナを実装し、その間にICチップを置き、外部アンテナと接続したICチップ付きテープの一例を示す構成図。

【図13】

テープに平行に二つの外部アンテナを実装し、その間にICチップを置き、外部アンテナと接続したICチップ付きテープの別形態の構成図。

【図14】

テープに平行に二つの外部アンテナを実装し、その間にICチップを置き、外部アンテナと接続し、ICチップの反対側からも外部アンテナと接続したICチップ付きテープの一例を示す構成図。

【図15】

ICチップ付きテープの一例の完成図。

【図16】

ICチップ付きテープを分断し、ICチップ付きタグとした例の説明図。

【図17】

証明書にICチップをテープ状にしたものをつけた証明書の一例の構成図

【図18】

ICチップをテープ状にして組み込んだ証明書に、ICチップの情報と金額情報を秘密鍵でデジタルサインをした結果を記載した証明書の一例を示す説明図。

【図19】

証明書にICチップを貼り付けた、あるいは埋め込んだ証明書の一例の構成図

【図20】

ICチップの情報と証明書番号情報を秘密鍵でデジタルサインをした結果を記

載したICチップ付きシールの一例を示す構成図。

【図21】

ICチップ付きシールをはがきにはさんで配布するための実装方法の一例を示す説明図。

【図22】

はがきにICチップチップを組み込んでICチップ付き証明書を配布するはがきの一例を示す説明図。

【図23】

ICチップ付きシールを貼った証明書の一例の構成図。

【図24】

ICカードチップ質問機兼用携帯電話の一例の外観図。

【図25】

ICカードチップ質問機兼用携帯電話の一例の構成図。

【図26】

文字情報読取兼用ICチップ質問機の一例の外観図。

【図27】

文字情報読取兼用ICチップ質問機の処理の例を示す図。

【図28】

簡易型証明書発行装置の一例の外観図。

【図29】

証明書を使ったサービスシステムの説明図。

【図30】

ICチップ付き証明書を使ったサービスシステムの一例の説明図。

【図31】

ICチップ付きシールを使ったサービスシステムの他の例の説明図。

【図32】

ICチップ付きシールを貼るための台紙の一例の外観図。

【図33】

ICチップの内容を外部から読み取ることを防ぐカードケースの一例の説明図

【図34】

利用権情報センターでICチップの正当性の確認を行うサービスシステムの一例の説明図。

【図35】

利用権情報センターで格納・管理を行う利用権情報に関するデータベースの一例の説明図。

【図36】

利用権情報センターあるいはサービス機関代行センターの一例の構成図。

【図37】

サービス実施機関における処理の例を示す図。

【図38】

利用権情報確認センターの処理部で行う正当性確認処理の一例の説明図。

【図39】

サービス機関代行センターでICチップの正当性の確認を行うサービスシステムの一例の説明図。

【図40】

ICチップ内の情報の例を示す図。

【図41】

ICチップ質問機兼用携帯電話の画面の一例を示す図。

【図42】

サービス機関代行センターで格納・管理を行う利用権情報に関するデータベースの一例の説明図。

【図43】

サービス機関代行センターでの正当性確認処理の一例の説明図。

【図44】

サービス機関代行センターでの利用者からの問い合わせに対する処理の一例の説明図。

【図45】

ICチップ発行センターとサービス機関からなるシステムの例を示す説明図。

【図46】

ICチップ発行センターが管理するICチップ番号とサービス機関の対応表の図。

【図47】

ICチップ発行センターとサービス機関、サービス機関代行センターからなるシステム例を示す説明図。

【符号の説明】

102 ICチップ

202 ICチップ付きシール

402 ICチップ付きテープ

502 ICチップ

504 電源部、論理部、メモリ部などを格納しているICチップの領域

506, 508 パッド部

602 ICチップ付きテープ

606, 608 外部アンテナ

702 ICチップ付きテープ

704, 706 ICチップ

708, 710, 712 外部アンテナ

802 外部アンテナ付きテープ

804, 806, 808 外部アンテナ

1002 ICチップ付きタグ

1004 ICチップ

1006, 1008 外部アンテナ

1112, 1114, 1116, 1118 導電性粒子の印刷部分

1202 ICチップ付きテープ

1204, 1206, 1208, 1210 ICチップ

1212, 1214 外部アンテナ

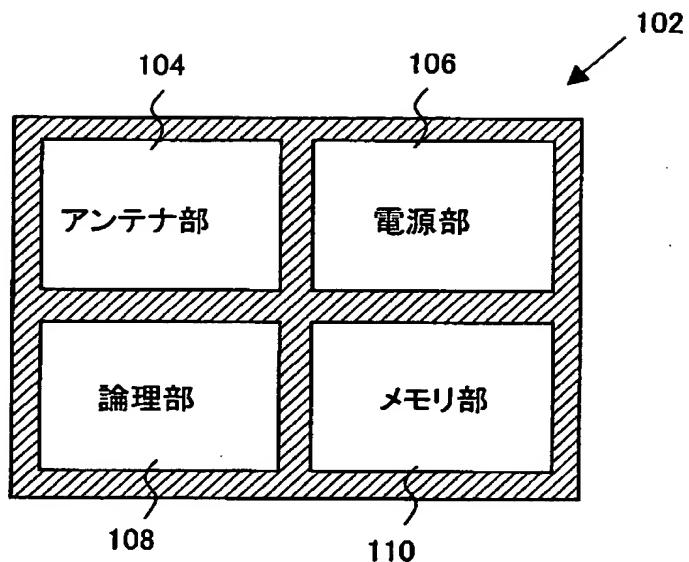
1302 ICチップ付きテープ

1304, 1306 ICチップ  
1308, 1310 外部アンテナ  
1408, 1410 外部アンテナ  
1502 ICチップ付きテープ  
1504, 1506 ICチップ  
1508, 1510 外部アンテナ  
1602 ICチップ付きタグ  
1604 ICチップ  
1606, 1608 外部アンテナ  
1702 ICチップ付きテープが貼られた証明書  
1704 ICチップ付きテープ  
1802 ICチップ付きテープが貼られた証明書  
1902 ICチップが組み込まれた、あるいは貼られた証明書  
1904 金額情報  
1906 デジタルサインの値  
1908 ICチップ  
2002 ICチップ付きシール  
2004 保険証番号  
2006 デジタルサインの値  
2008 ICチップ  
2102 二つ折りのはがきにICチップ付きシールをはさんで圧着したはがき  
2104 ICチップ付きシール  
2302 ICチップ付きシールが貼られた証明書  
2304 保険証番号  
2306 デジタルサインの値  
2308 ICチップ付きシール  
2402 ICチップ付きシール  
2406 ICカードチップ質問機兼用携帯電話  
2412 ICカードチップ質問機機能と携帯電話機能を切り替えるスイッチ

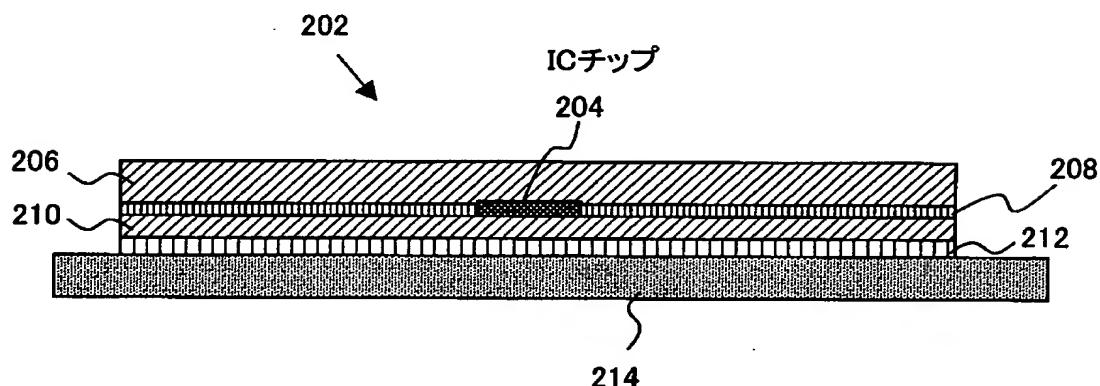
- 2514 スイッチ部  
2608 文字情報読取兼用 ICチップ質問機  
2806 ICチップ書き込み部  
2814 簡易型証明書発行装置  
3202 ICチップ付きシールを貼るための台紙  
3204 ICチップ付きシール  
3206 ICチップ付きシールを貼る窪み  
3208 ICチップ付きシールを貼る窪み  
3302 ICチップの内容を外部から読み取ることを防ぐカードケース  
3304, 2106 金属膜  
3502 ICチップの正当性を確認するためのデータベース  
4202 ICチップの正当性を確認するためのデータベース

【書類名】 図面

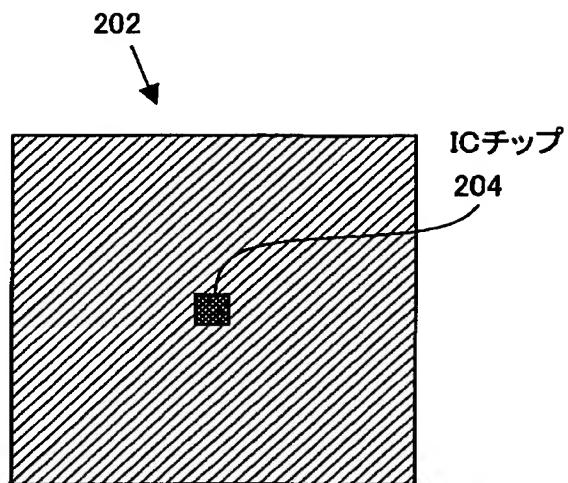
【図1】



【図2】



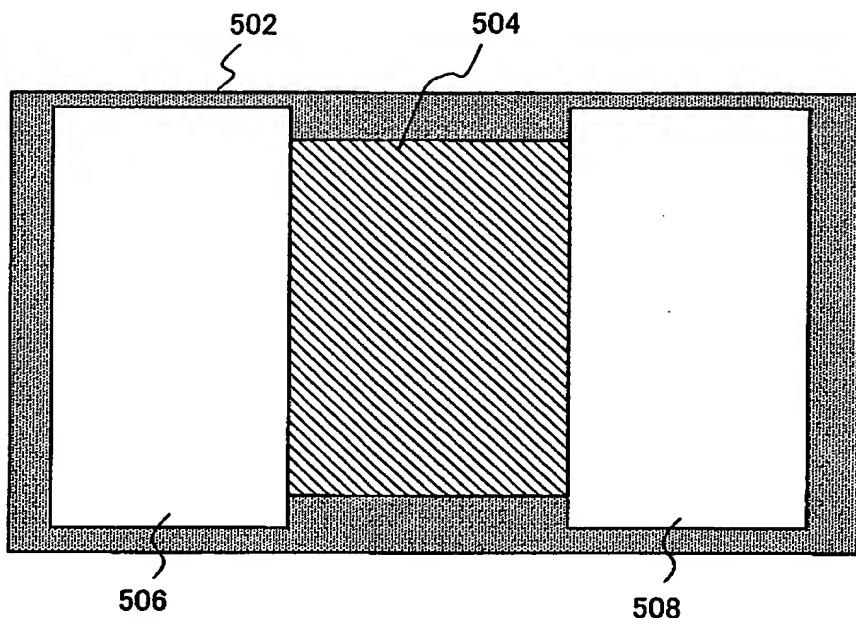
【図3】



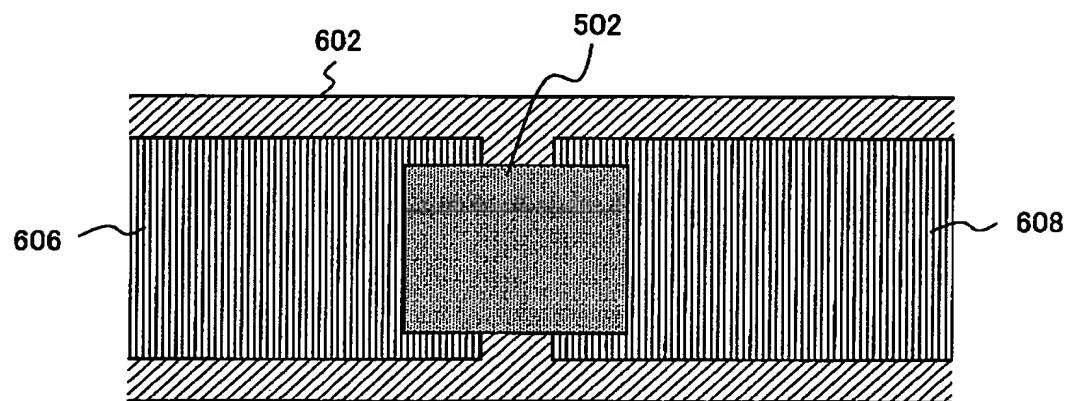
【図4】



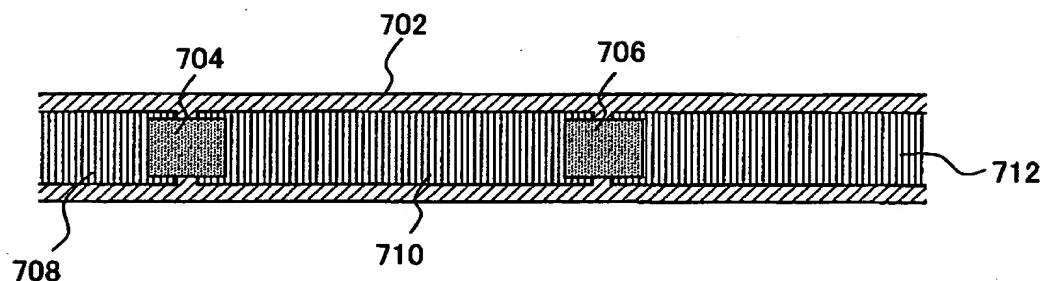
【図5】



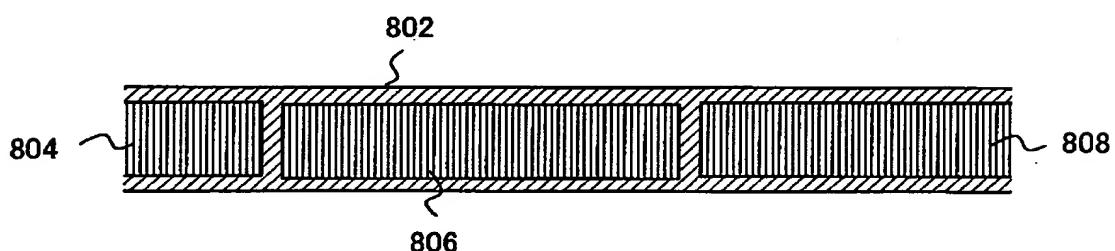
【図6】



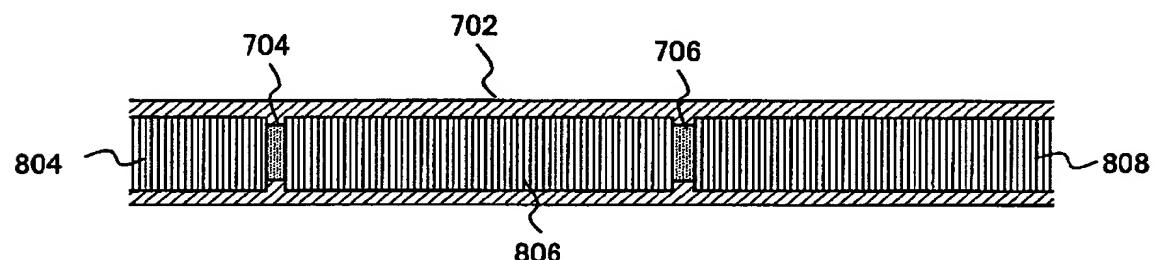
【図7】



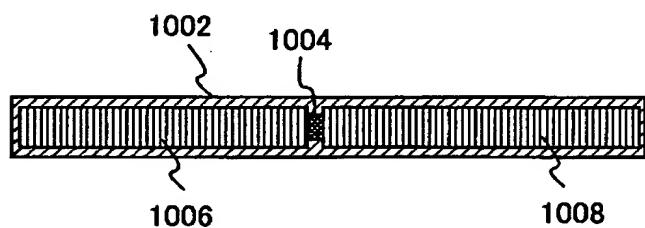
【図8】



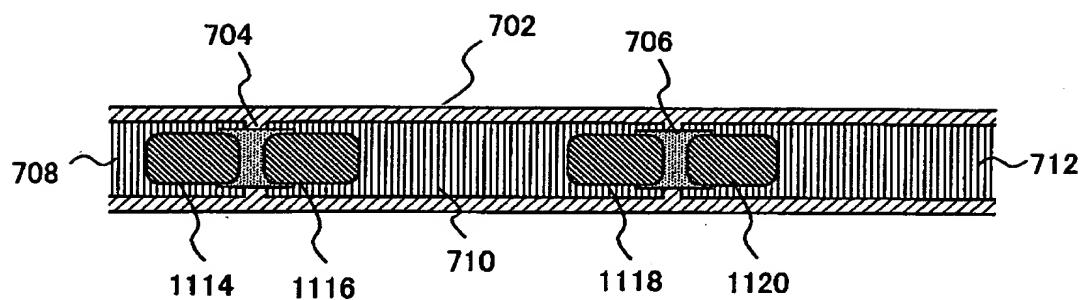
【図9】



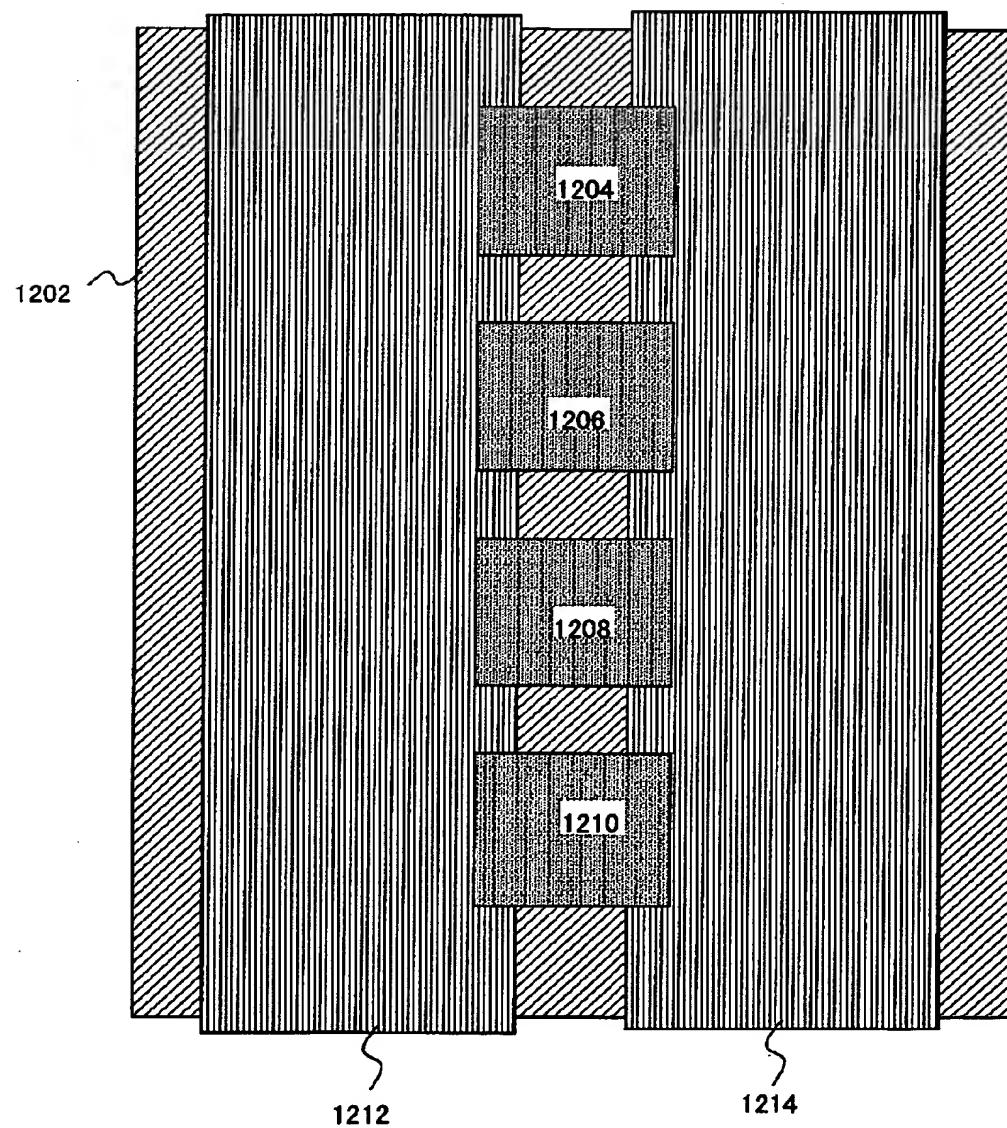
【図10】



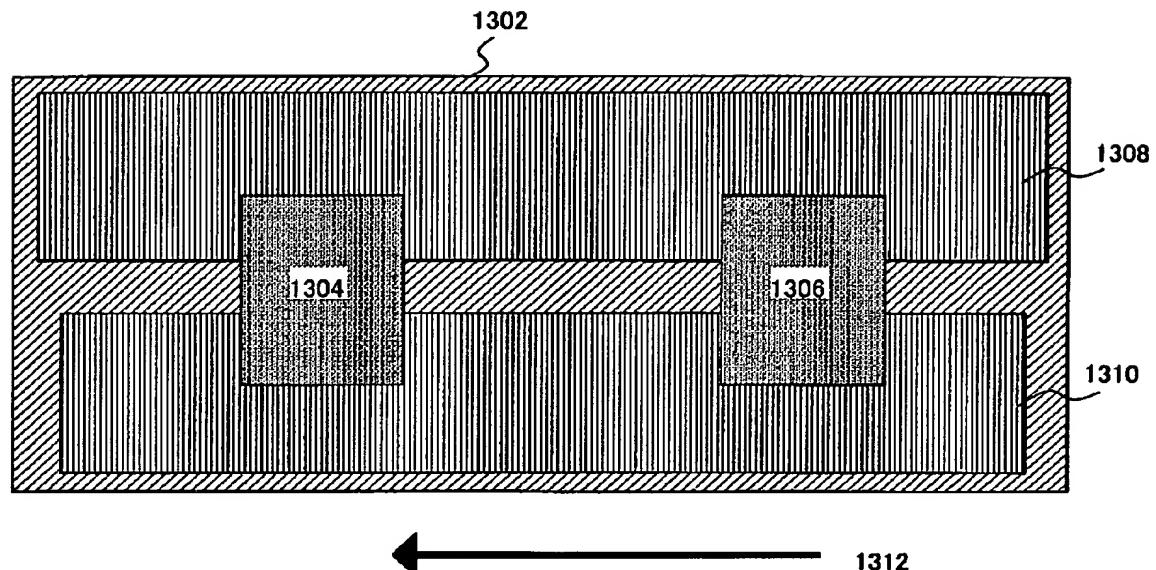
【図11】



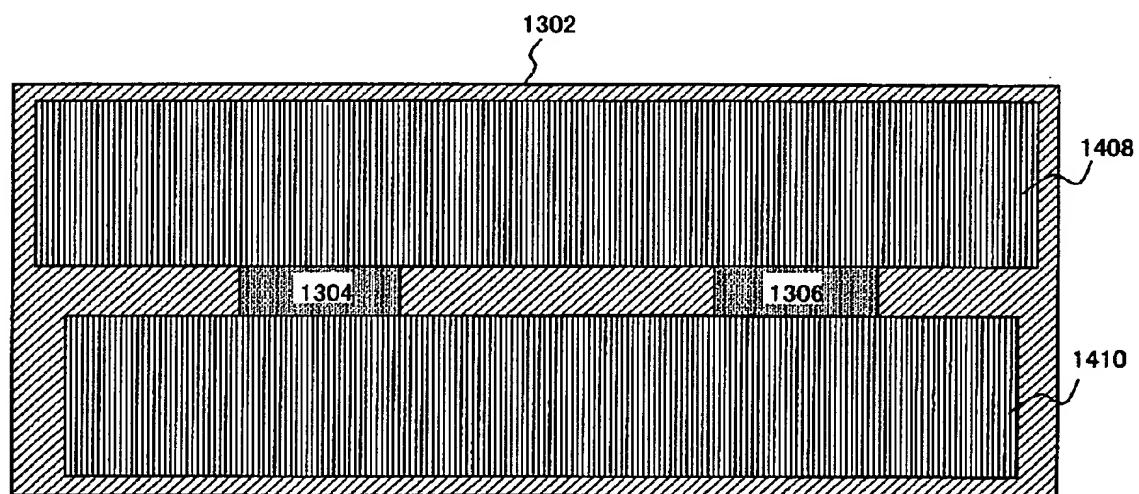
【図12】



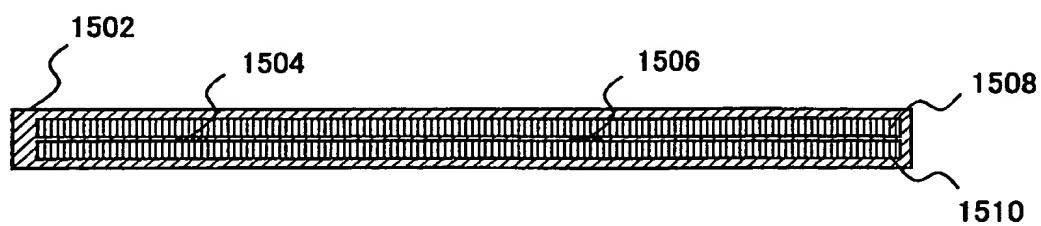
【図13】



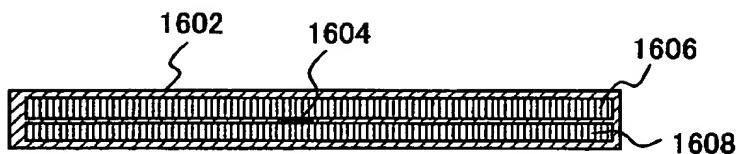
【図14】



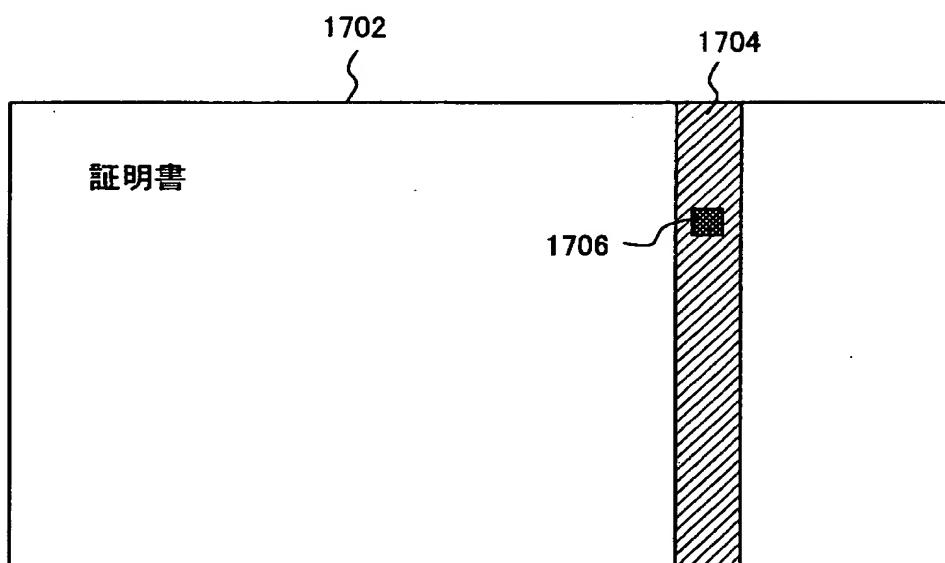
【図15】



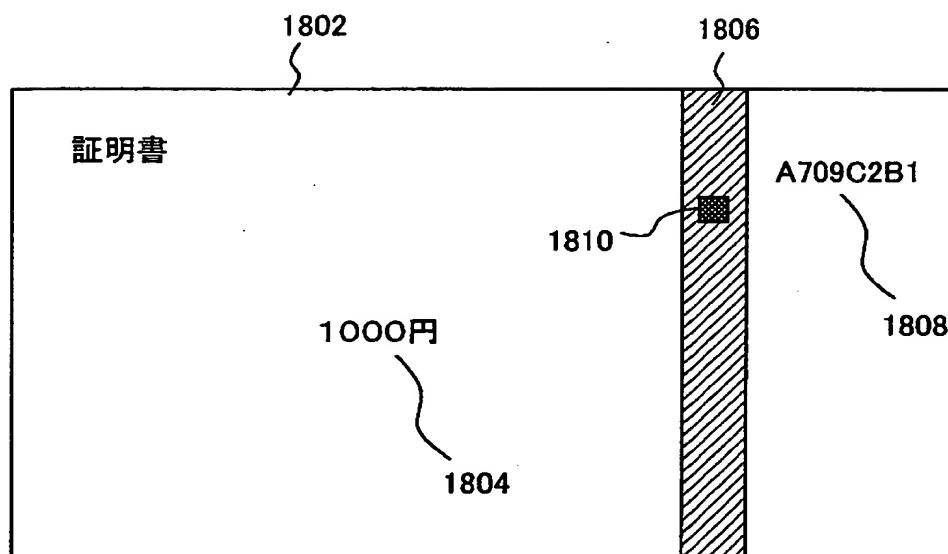
【図16】



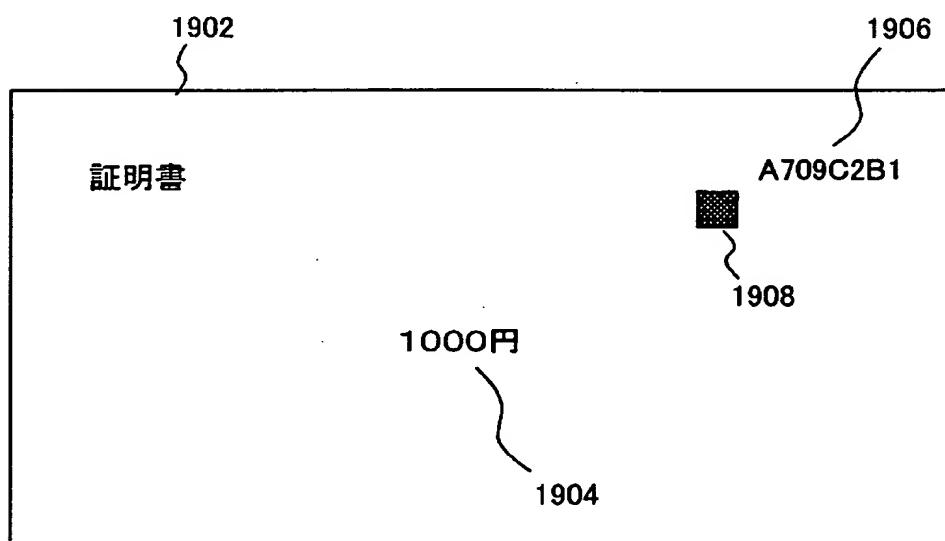
【図17】



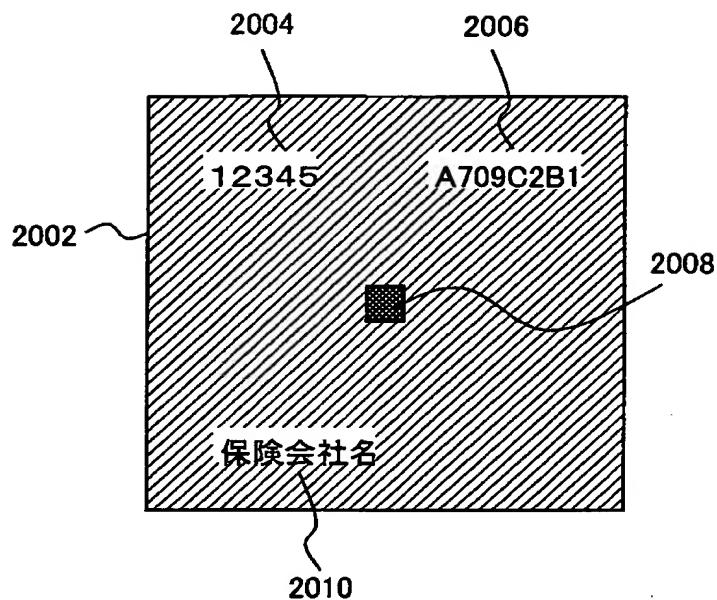
【図18】



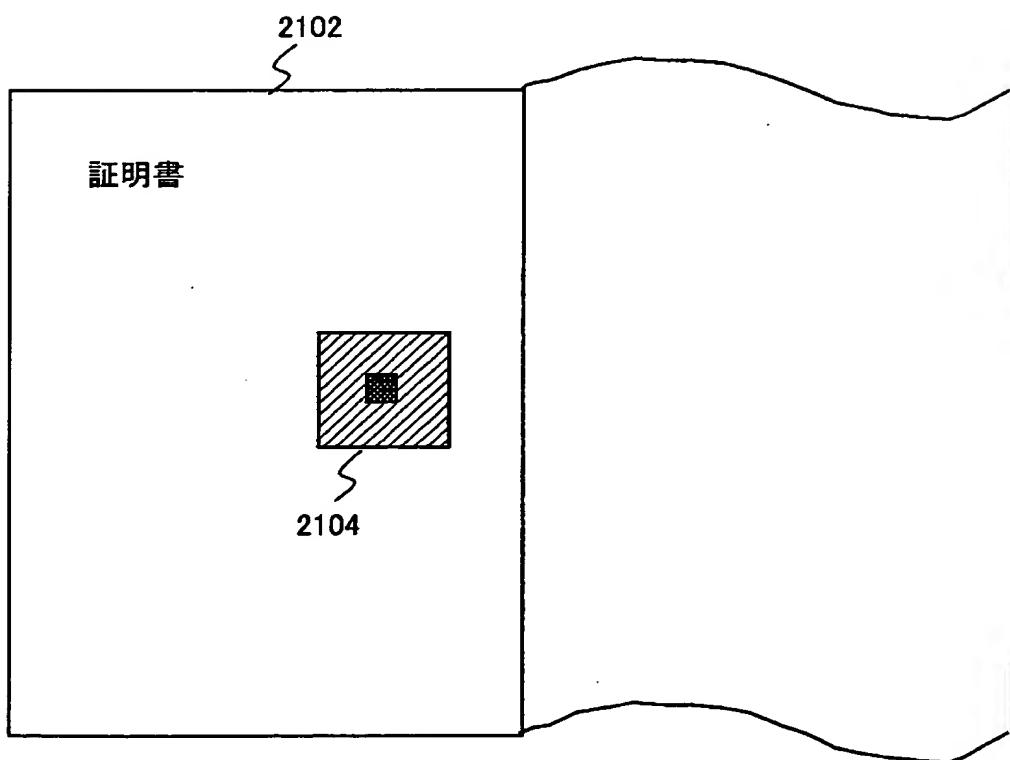
【図19】



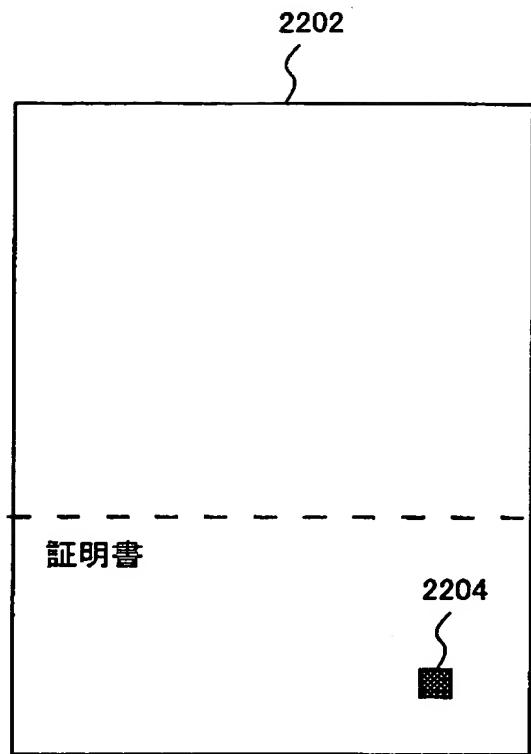
【図20】



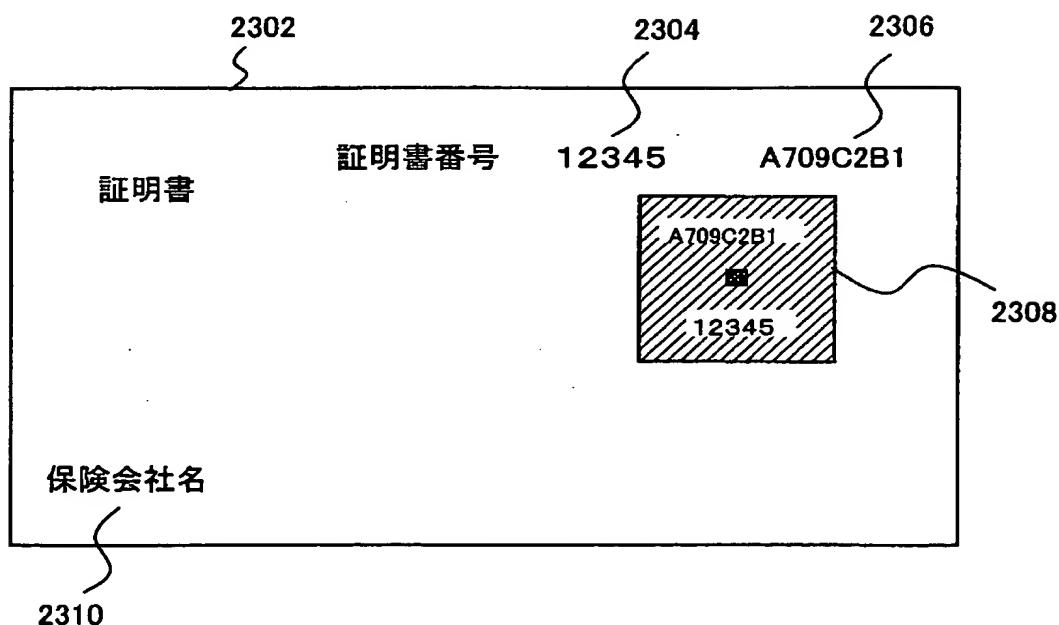
【図21】



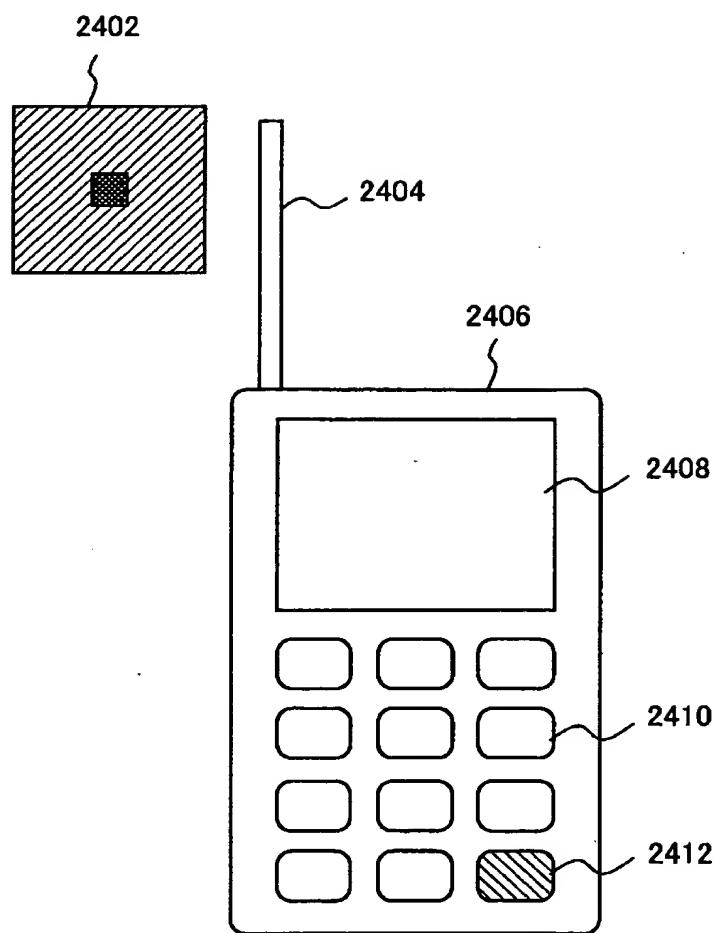
【図22】



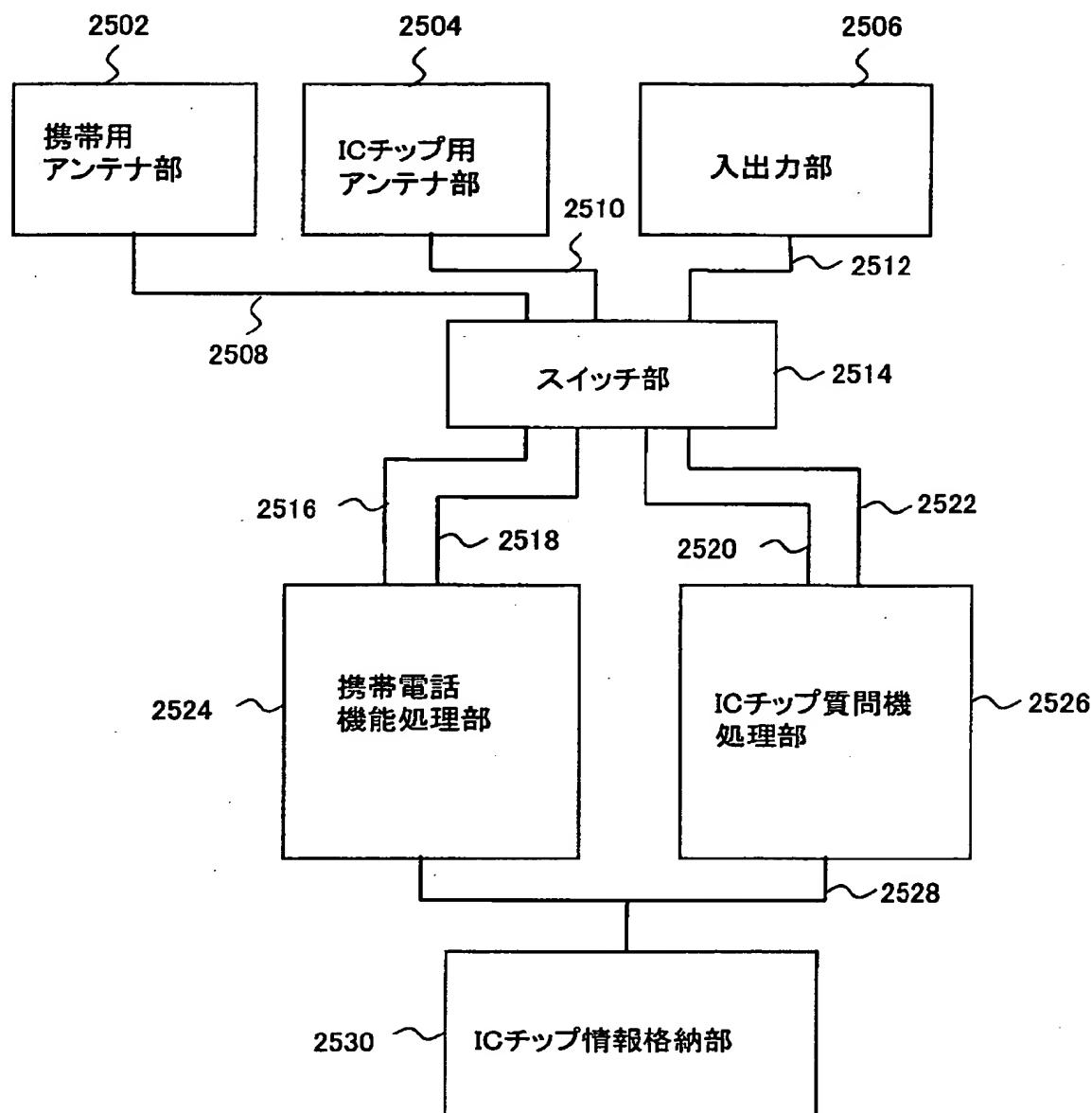
【図23】



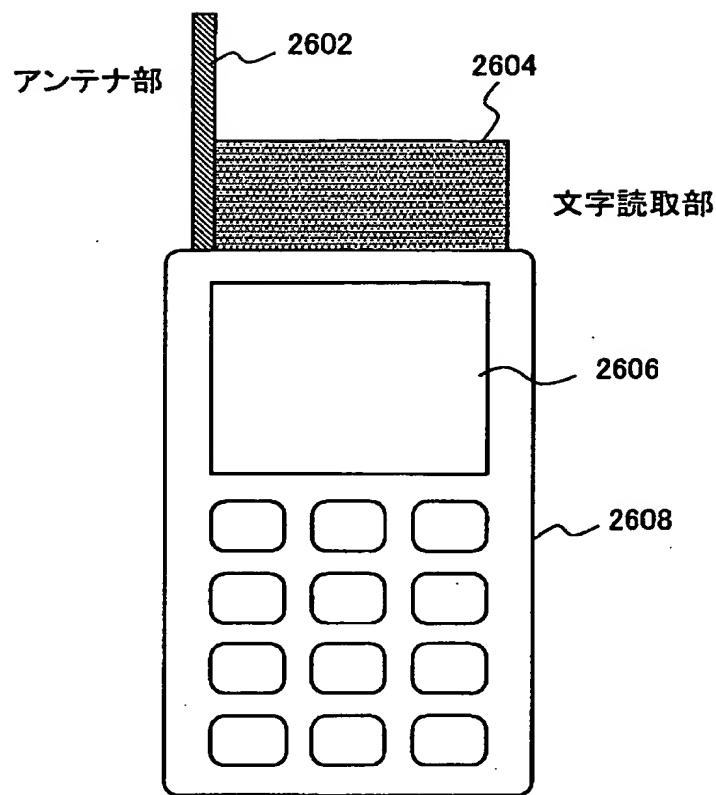
【図24】



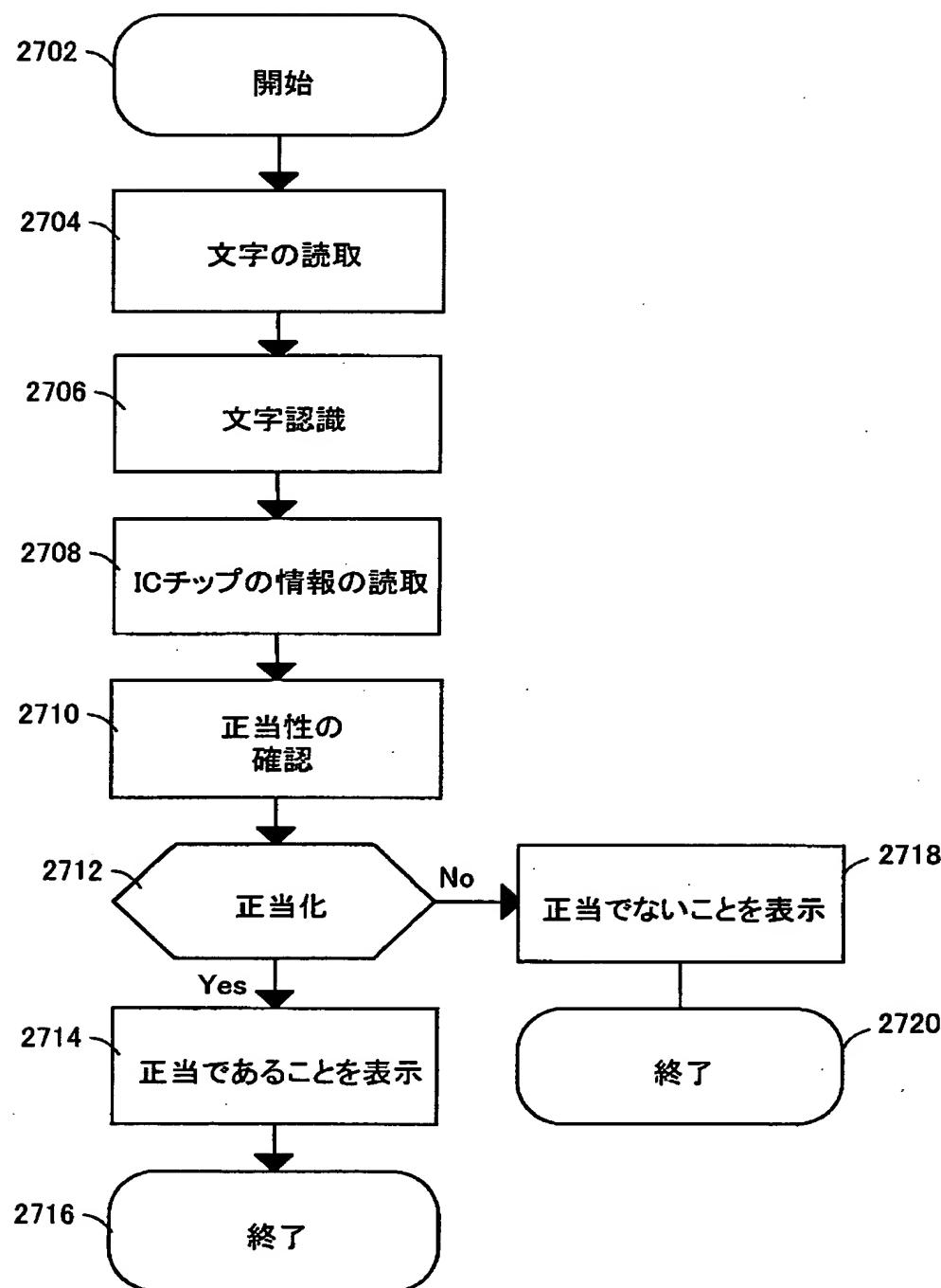
【図25】



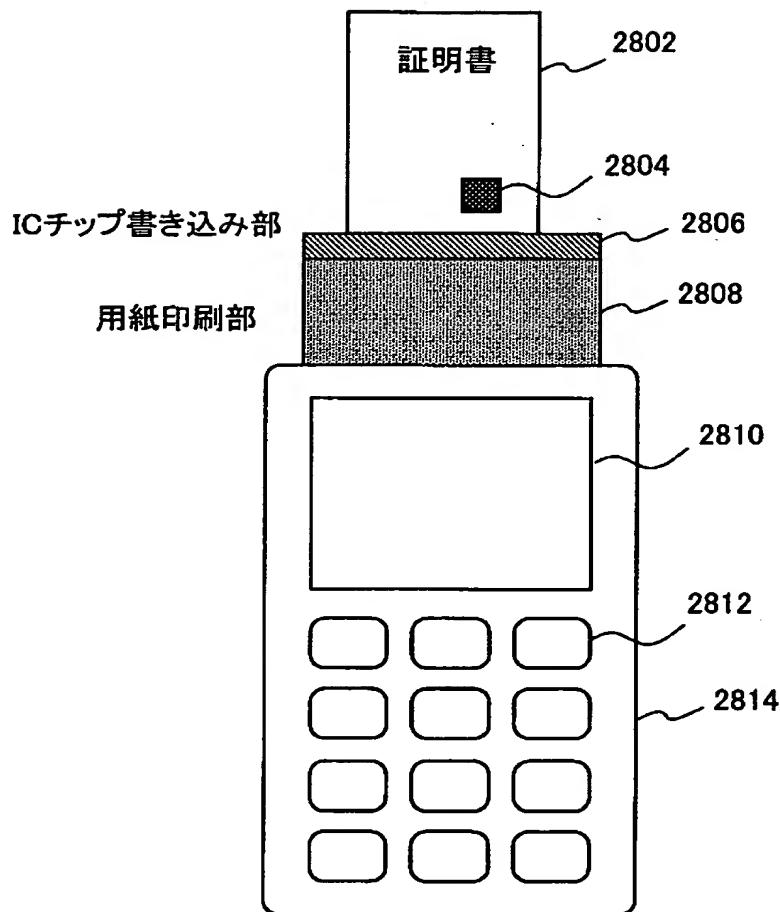
【図26】



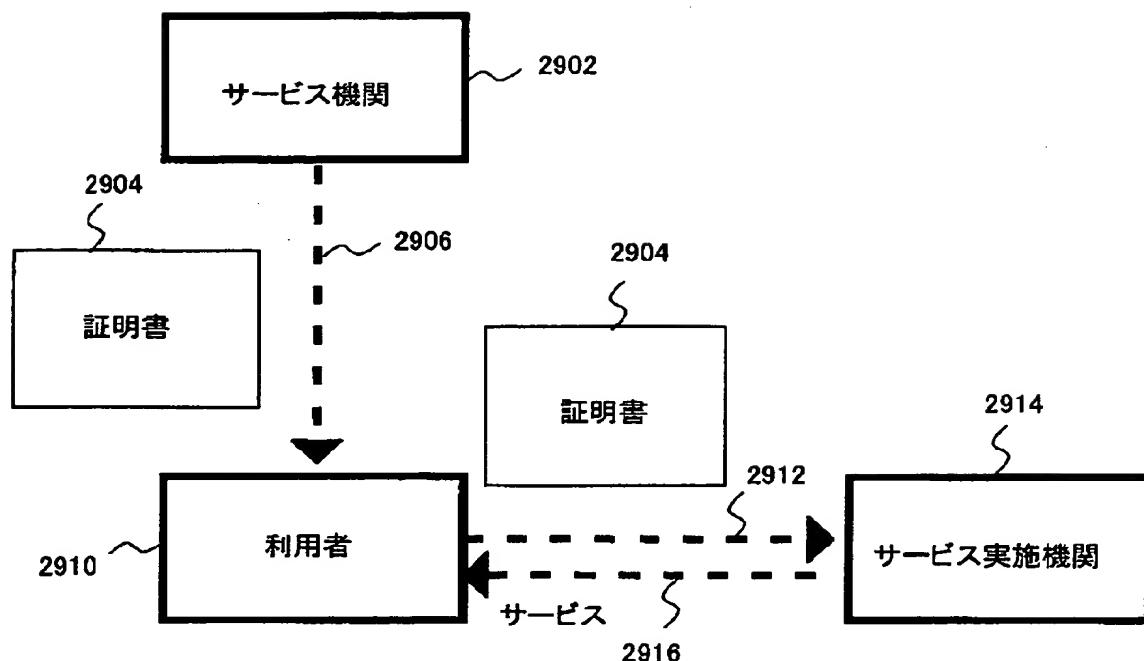
【図27】



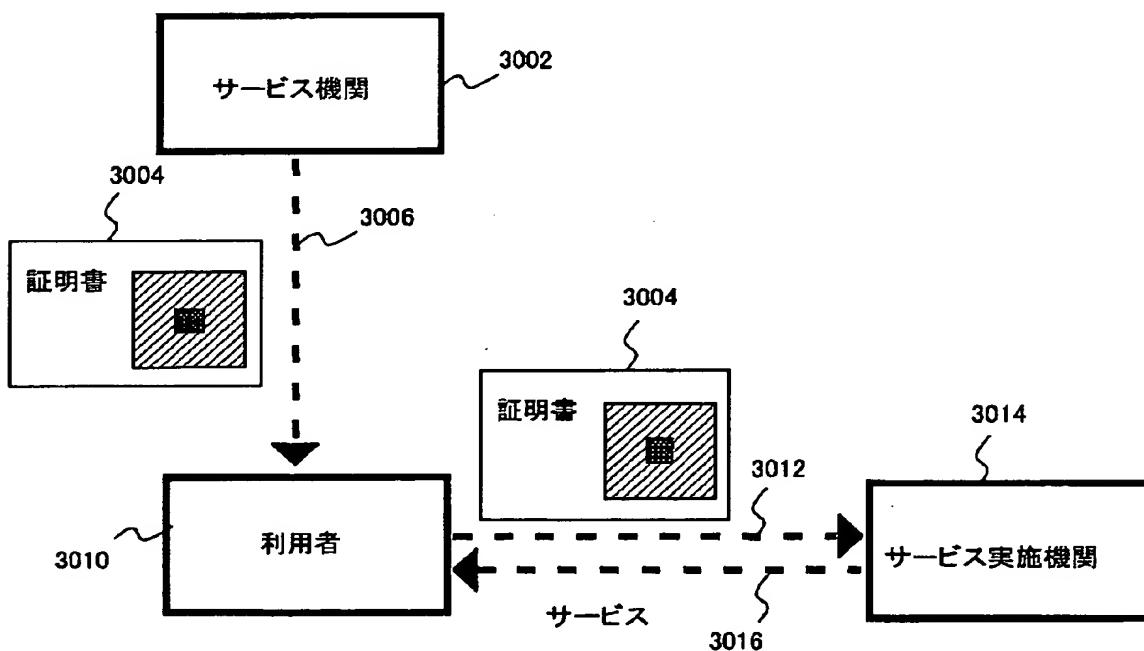
【図28】



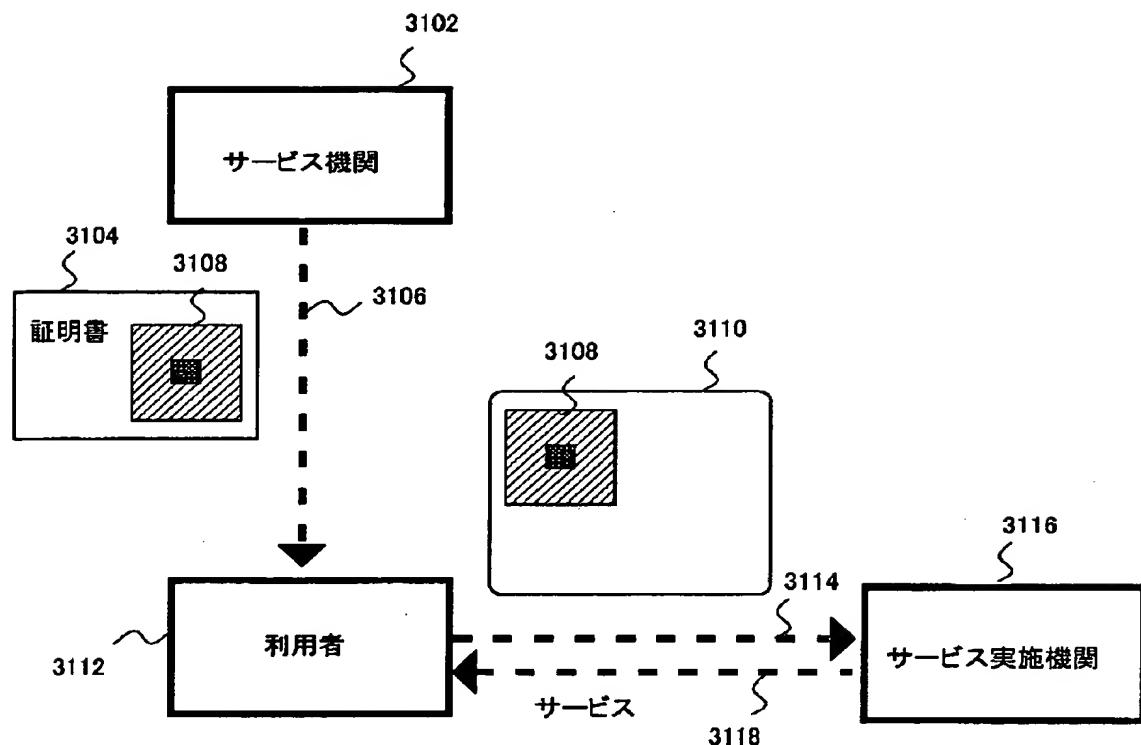
【図29】



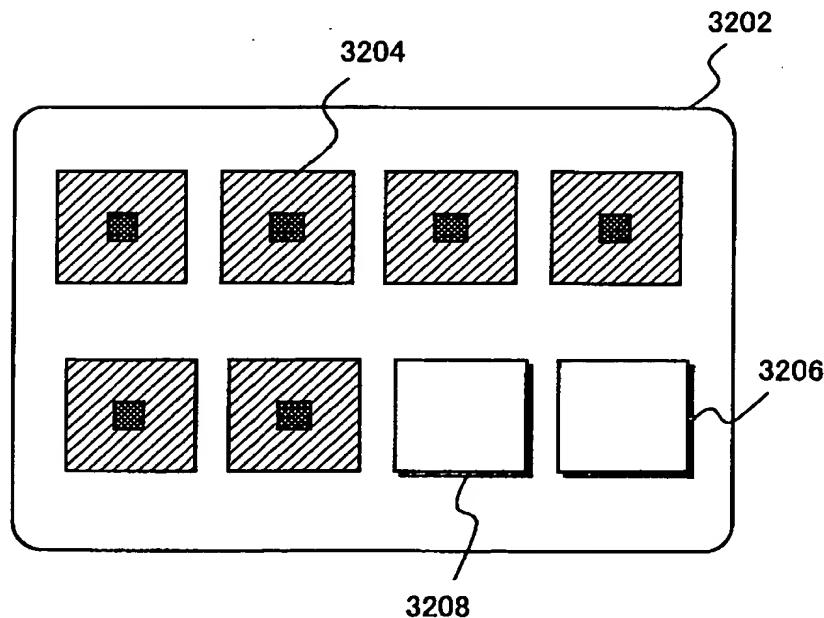
【図30】



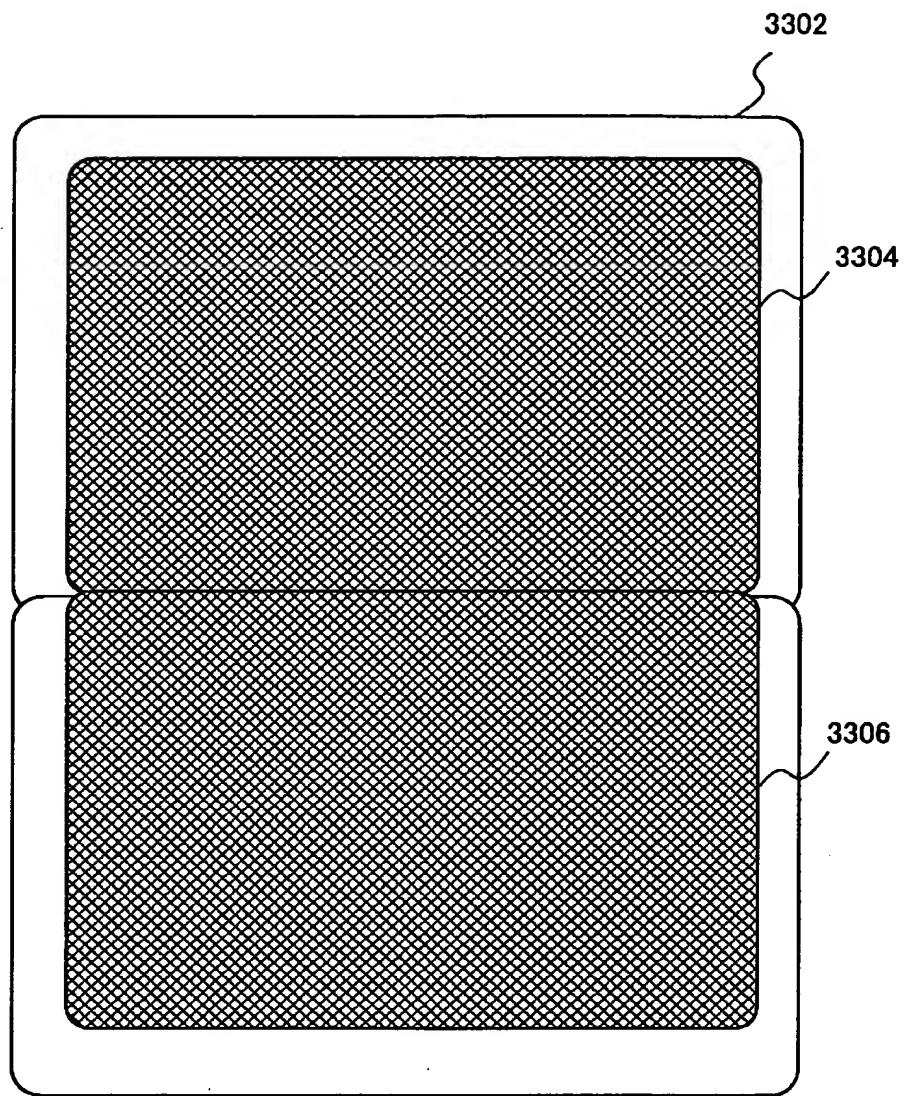
【図31】



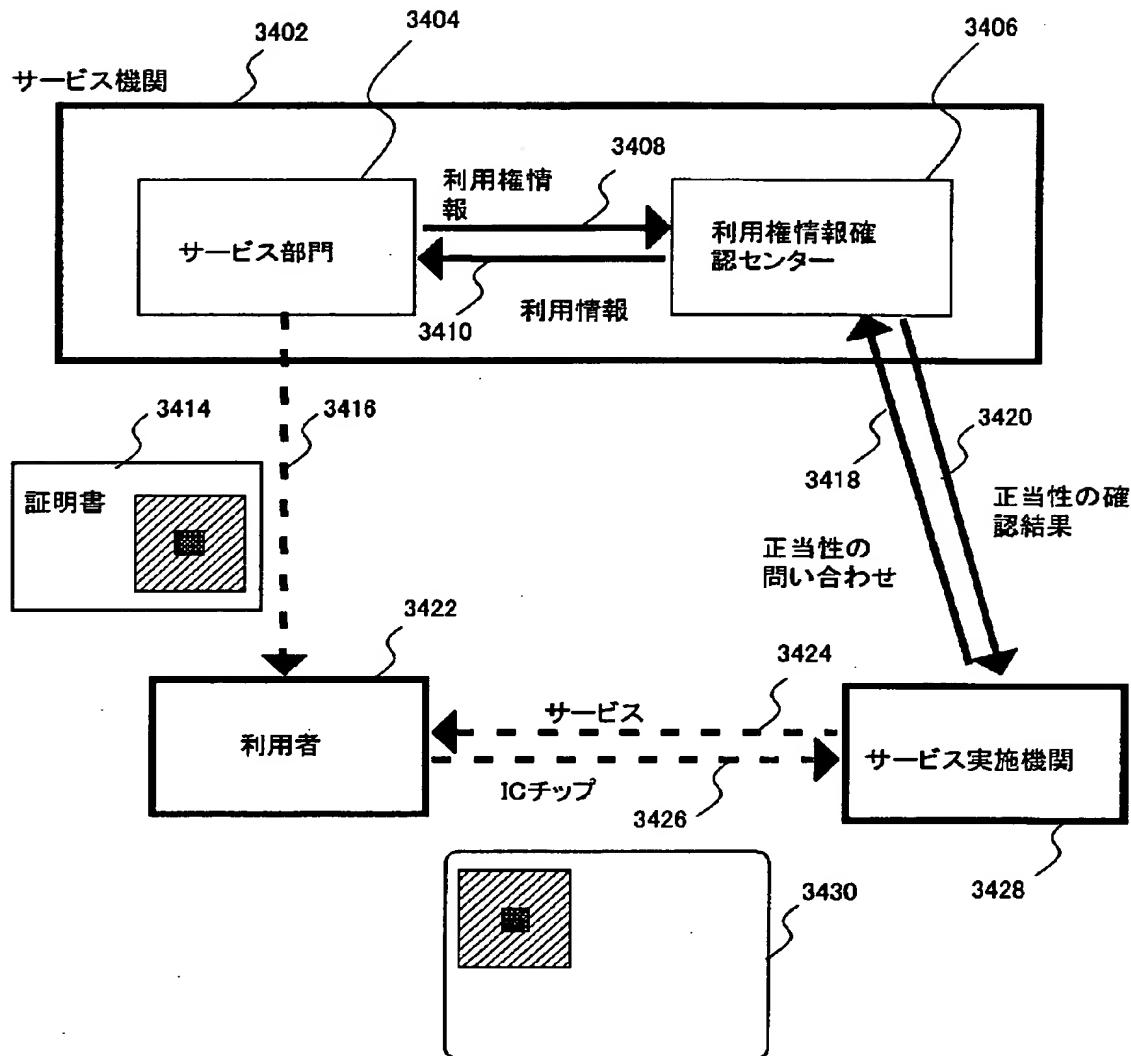
【図32】



【図33】



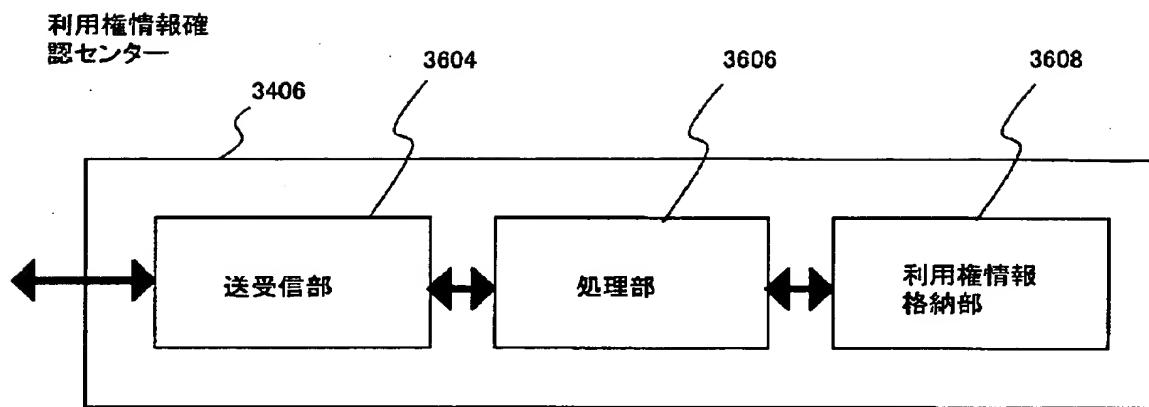
【図34】



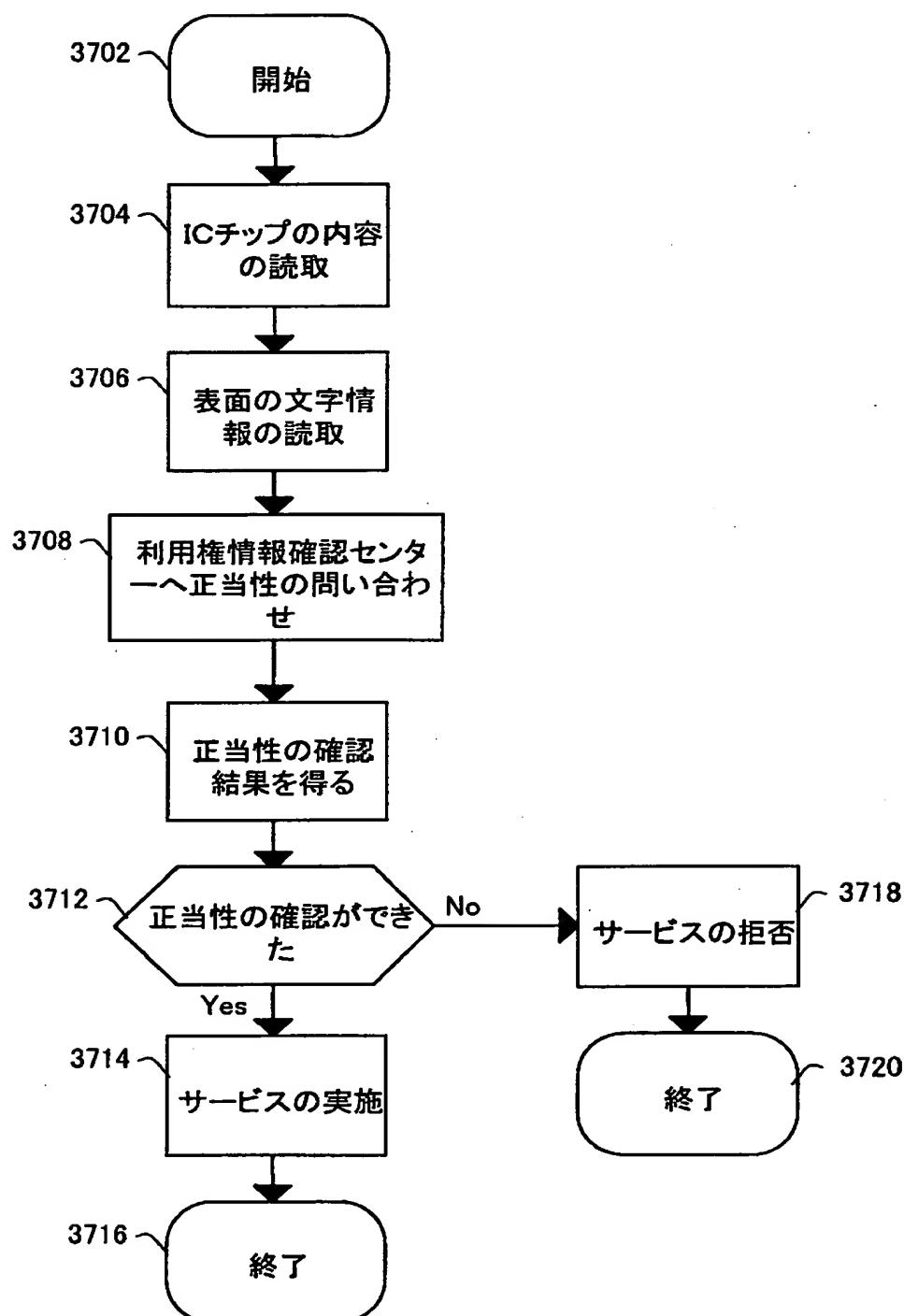
【図35】

ICチップ番号 3502	利用者情報 3504	正當性確認情報 3506	サービス内容 3508	利用状況 3510	有効期限 3512	3514

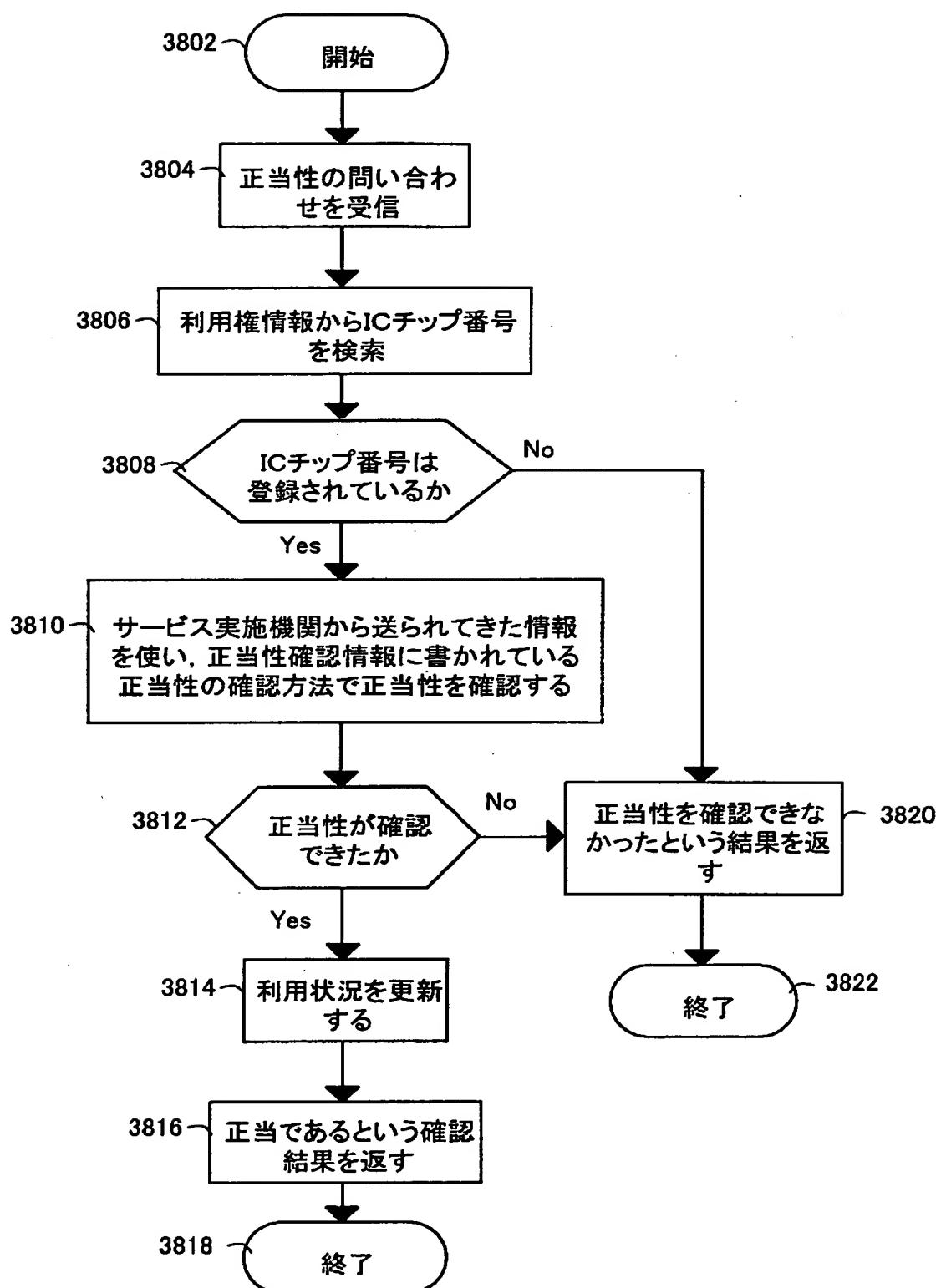
【図36】



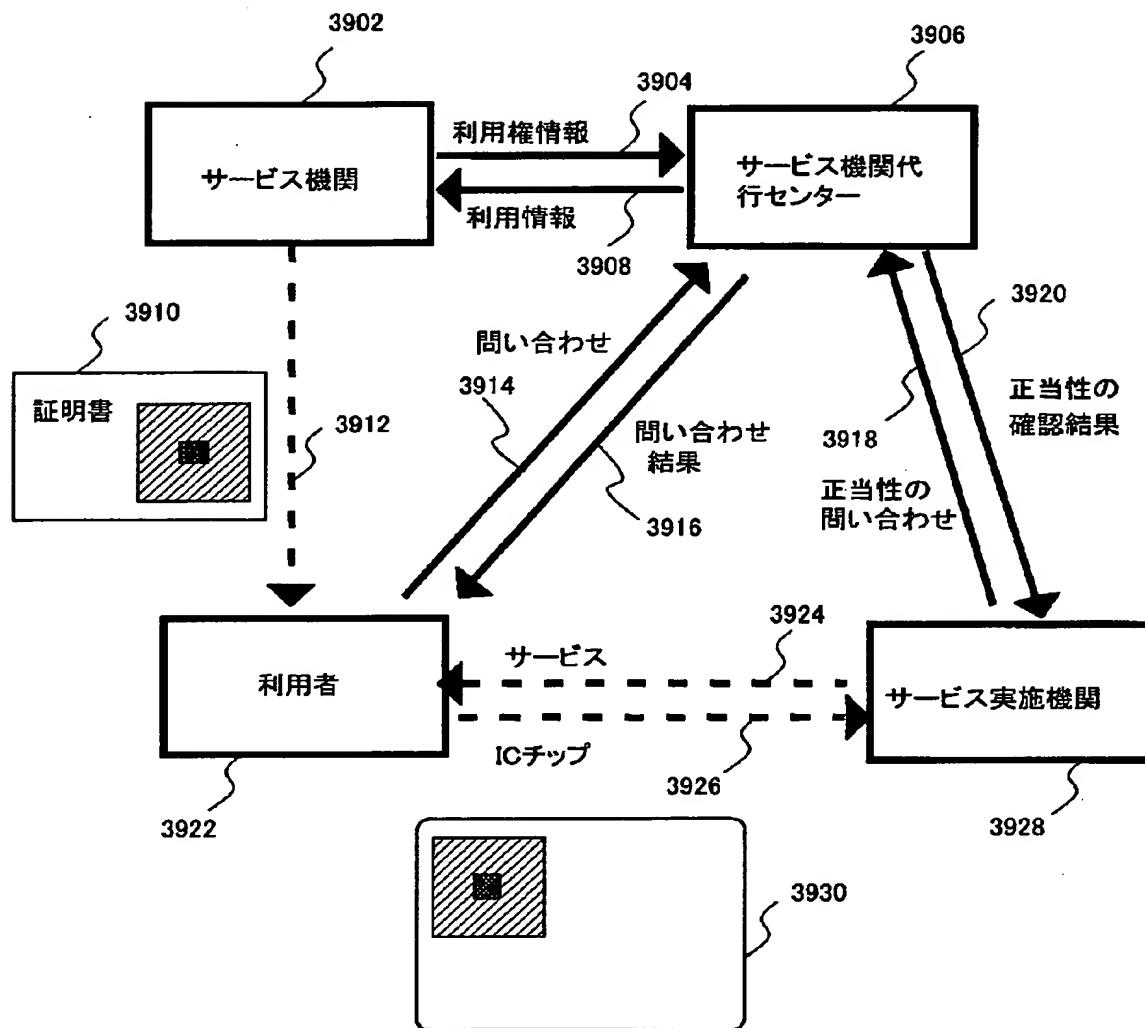
【図37】



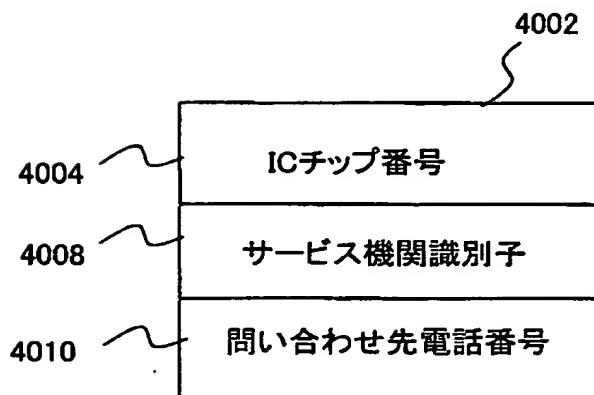
【図38】



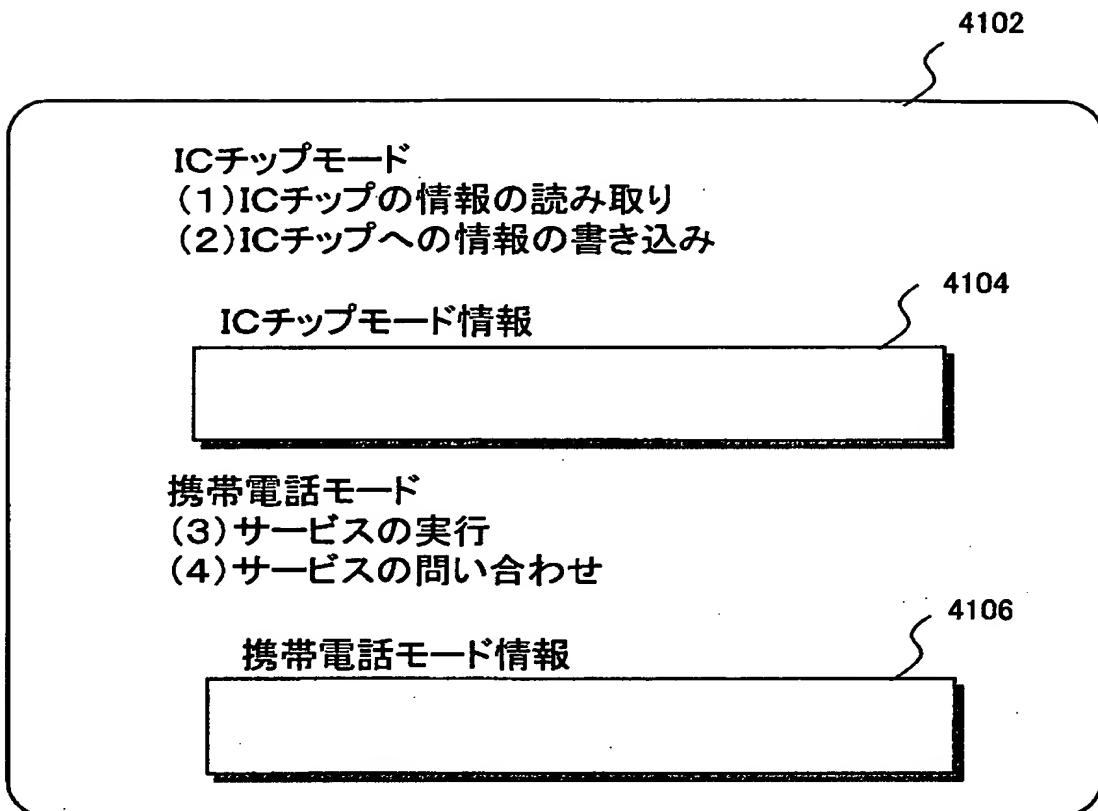
【図39】



【図40】



【図4-1】



【図4-2】

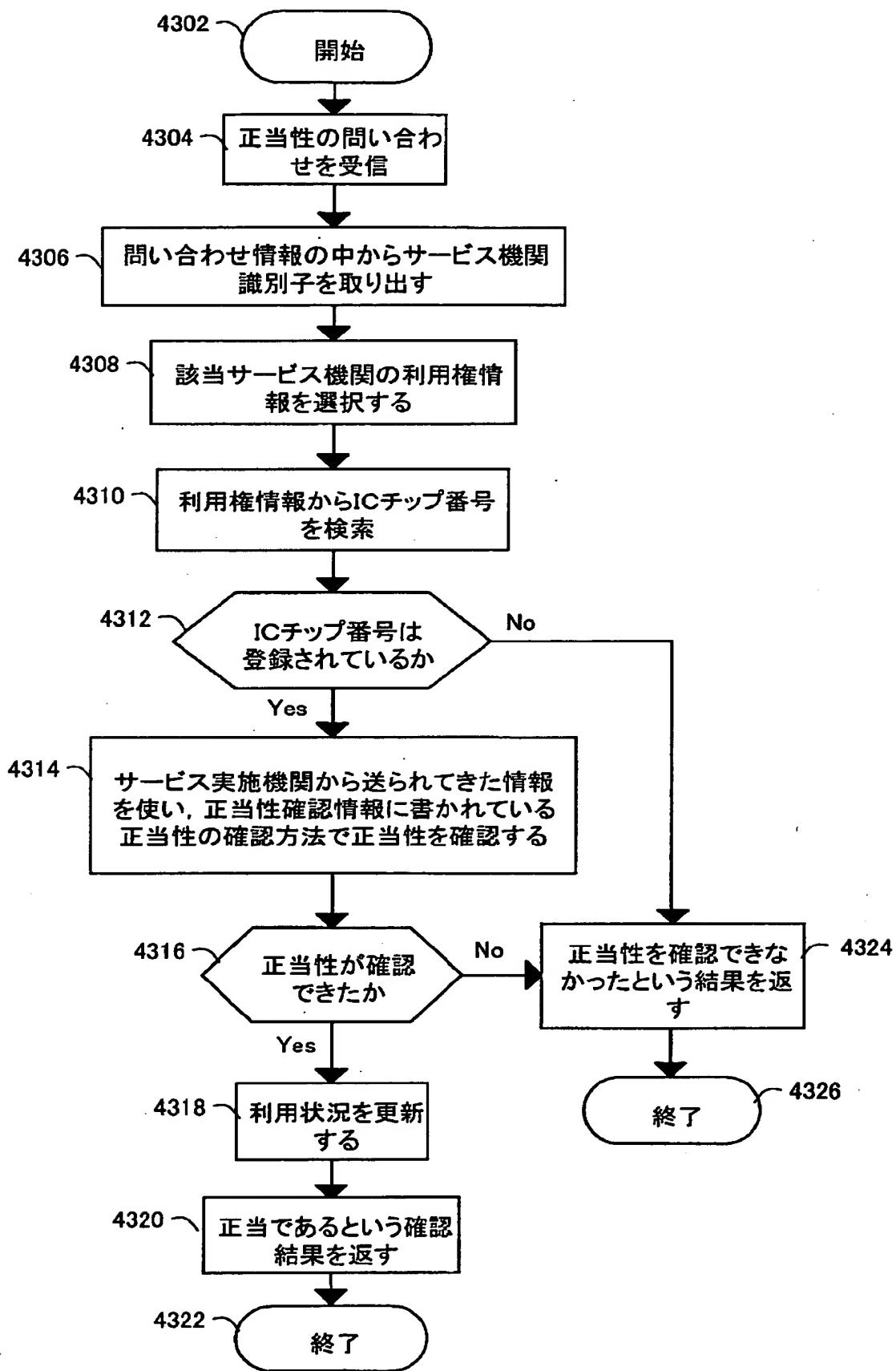
サービス機関A

ICチップ番号	利用者情報	正当性確認情報	サービス内容	利用状況	有効期限

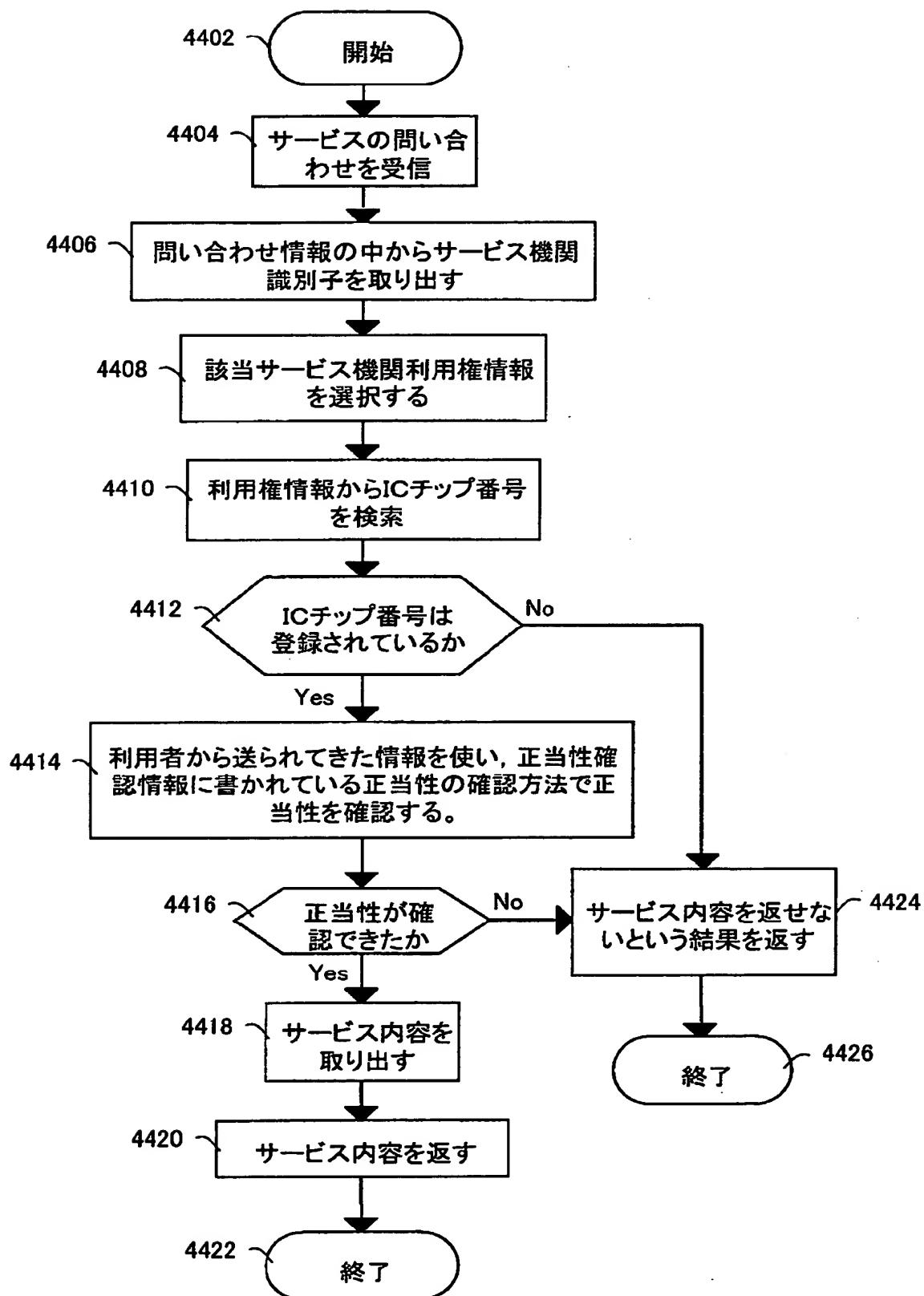
サービス機関B

ICチップ番号	利用者情報	正当性確認情報	サービス内容	利用状況	有効期限

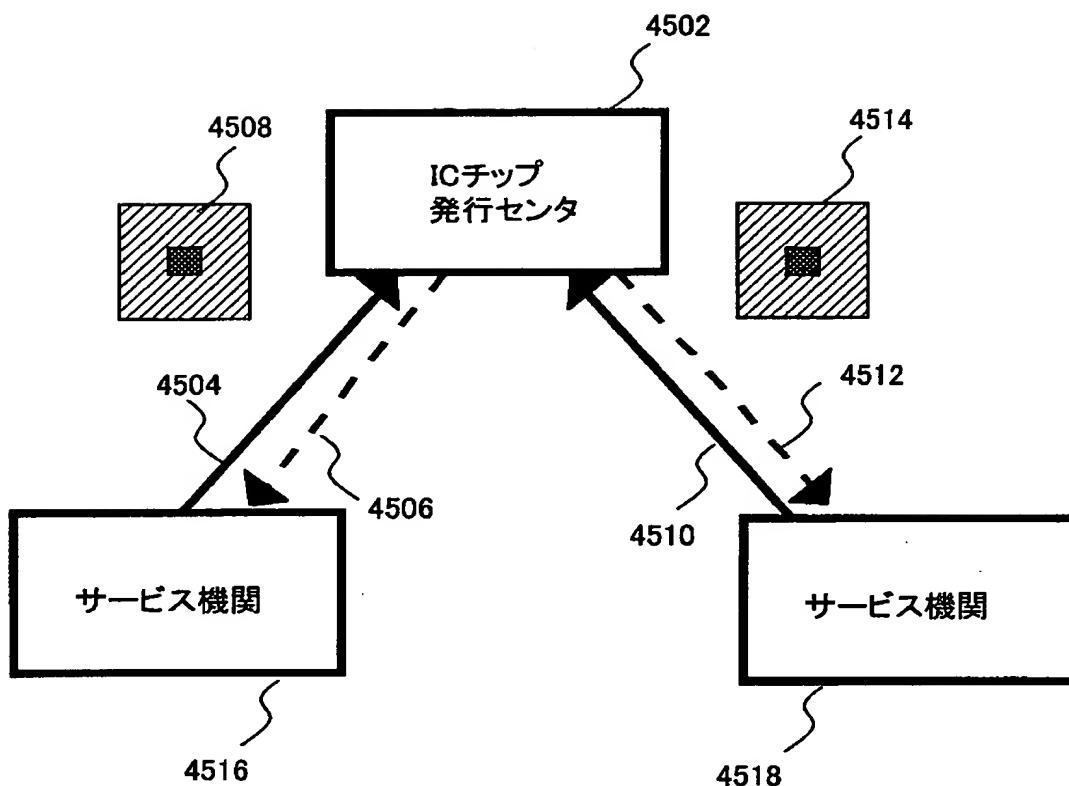
【図4-3】



【図44】



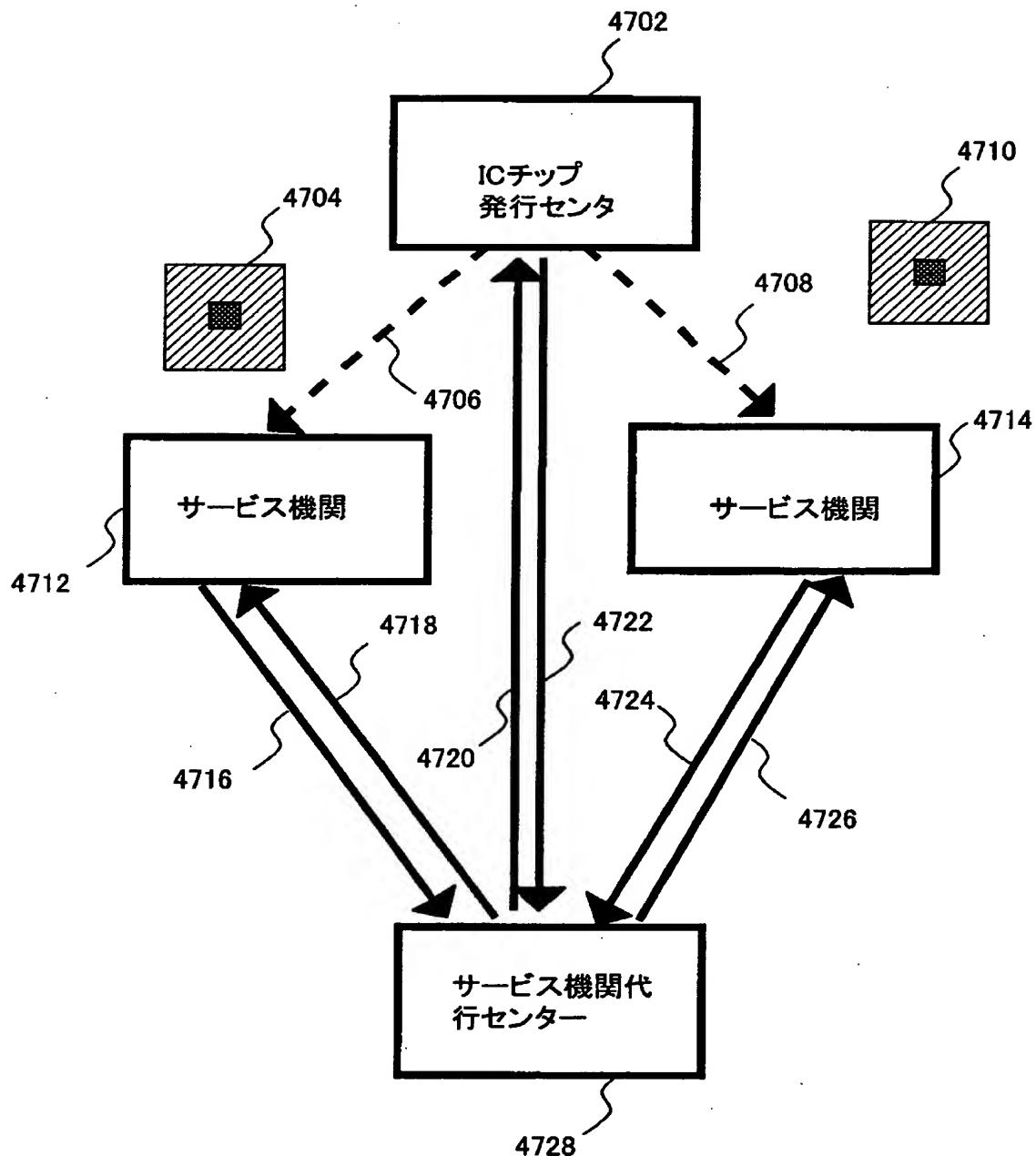
【図45】



【図46】

ICチップ番号	サービス機関

【図47】



【書類名】 要約書

【要約】

【課題】 持ち運びに便利で偽造の困難な証明書を用いたサービスシステムを提供する。

【解決手段】 携帯用の証明書として、非接触 ICチップを使用する。ICチップ付きシールは薄くて小さいため、配布も携帯も容易である。証明書3910にICチップを組み込んだり、貼ることにより、偽造を困難にする。

【選択図】 図39

出願人履歴情報

識別番号 [000005108]

1. 変更年月日 1990年 8月31日

[変更理由] 新規登録

住 所 東京都千代田区神田駿河台4丁目6番地  
氏 名 株式会社日立製作所